



Nota informativa

Ha culminado una inspección sectorial de oficio sobre el empleo de cámaras que permiten difundir imágenes en Internet

La AEPD alerta de los riesgos por la utilización de cámaras de vigilancia que emiten a través de internet sin controles de acceso

- Se trata de cámaras conectadas a Internet que permiten un acceso remoto a través de la Red al visionado de las imágenes en tiempo real.
- Se ha detectado que parte importante de estas cámaras carecen de controles de acceso y captan y difunden imágenes de personas identificables en la vía pública, el lugar de trabajo o en el interior de establecimientos comerciales.
- Se ha comprobado que la visualización de las imágenes captadas puede hacerse desde cualquier ordenador conectado a Internet, y en algunos casos se permite incluso manejar remotamente la cámara y grabar las imágenes.
- Se han iniciado 7 procedimientos sancionadores, a particulares y a empresas por la captación de imágenes de personas identificables accesibles a cualquier usuario en Internet.
- El plan alerta de que el riesgo de acceso por parte de intrusos es muy elevado debido a la existencia de buscadores que, al rastrear periódicamente la Red, proporcionan mecanismos de búsqueda muy eficaces.

(Madrid, 1 de julio de 2009). La Agencia Española de Protección de Datos (AEPD) ha culminado una inspección sectorial de oficio sobre **videocámaras conectadas a Internet que permiten un acceso remoto a través de la Red al visionado de las imágenes en tiempo real** (cámaras IP), en el que ha constatado que, con demasiada frecuencia, quienes compran e instalan este tipo de dispositivos lo hacen sin activar los controles de acceso, ni cambian los usuarios y contraseñas que estos dispositivos traen por defecto.

Ante la proliferación de este tipo de dispositivos, y los posibles riesgos para la privacidad, la AEPD decidió analizar la problemática asociada a la utilización de este tipo de sistemas. Para ello ha realizado una inspección sectorial de oficio en la que se analiza este fenómeno y se **proporcionan recomendaciones y pautas de utilización que permitan el empleo de este tipo de dispositivos dentro del marco de la normativa de protección de datos**. Para su realización se han analizado webs que captan imágenes de paisajes o panorámicas, de la vía pública, de lugares de trabajo y del interior de establecimientos comerciales.

Entre las principales situaciones detectadas se ha constatado que existen muchos casos en los que las cámaras que emiten imágenes a través de Internet únicamente recogen **paisajes o panorámicas** que, al no recabar imágenes de personas que pudieran ser identificadas o reconocidas, no presentan riesgo para la privacidad.

No obstante la AEPD ha constatado que **buena parte de las cámaras que emiten imágenes a través de la Red, las captan de la vía pública, el lugar de trabajo o el interior de**

establecimientos comerciales, si que permiten la identificación de personas y carecen de control de acceso, es decir, que difunden imágenes en abierto, con el impacto que ello supone para la privacidad y el alto riesgo de incumplimiento de la normativa de protección de datos.

Asimismo, se ha constatado que incluso algunas de las cámaras pertenecen a personas físicas que, sin el soporte de una organización o empresa, han instalado dichos dispositivos a título individual, difundiendo a través de Internet las imágenes captadas.

Fruto de la situaciones detectadas en el transcurso de esta inspección la AEPD **ha iniciado 7 procedimientos sancionadores, en los que el elemento común es la captación de imágenes de personas identificables que se encontraban accesibles a cualquier usuario en Internet**. En dos de los casos, son particulares los que captaban y por tanto permitían visualizar, imágenes en la vía pública sin consentimiento de los afectados, mientras que en el resto, son empresas que han captado (y permitido visualizar) en sus propios locales imágenes de los empleados o de terceras personas ajenas a la empresa, sin su consentimiento. La LOPD tipifica estas conductas como infracción grave.

La AEPD destaca en la inspección sectorial que la visualización de las imágenes captadas por la cámara puede hacerse desde cualquier ordenador conectado a Internet, **siempre que no se hayan establecido controles de acceso a la misma**. Y no sólo se puede acceder al visionado, sino que en ocasiones también se puede manejar remotamente la cámara (zoom, moverla en sentido horizontal y vertical, sonido e incluso grabar las imágenes recibidas).

Se ha detectado que, pese a que estas cámaras disponen de mecanismos de control de acceso basados en usuario y clave o contraseña, **es habitual que vengan desactivados de fábrica o vengan activados con usuarios y contraseñas por defecto**. Además, como se ha como se ha analizado, es demasiado frecuente que las personas que compran estas cámaras no activen dichos controles o no cambien las claves que vienen por defecto, lo que crea vulnerabilidad al dejar a la cámara en una situación de “puertas abiertas”.

Aunque esta situación pudiera considerarse de riesgo limitado, **el plan alerta de que, en la práctica, el riesgo es muy elevado debido a la existencia de buscadores**, que rastrean periódicamente la Red permitiendo el acceso a este tipo de sistemas y proporcionando mecanismos de búsqueda muy eficaces, que en sí misma proporciona mecanismos de búsqueda muy eficaces.

Decálogo de uso

La AEPD ha elaborado un decálogo con recomendaciones para que la utilización de las cámaras que emiten a través de Internet se haga conforme a la normativa de protección de datos. Destacan, entre otras:

1. Es esencial activar el control de acceso a las imágenes con usuario y contraseña. Formar al personal que las utiliza.
2. Recordar tanto a particulares como a empresas que la utilización de videocámaras para vigilar la vía pública está reservada únicamente a las Fuerzas y Cuerpos de Seguridad del Estado.
3. Hay que tener en cuenta que si se van a usar videocámaras por motivos de seguridad privada, éstas sólo podrán ser instaladas por empresas autorizadas por el Ministerio del Interior.
4. Si capta de imágenes panorámicas, -paisajes, edificios, tráfico urbano etc.-, asegúrese de que nunca se tomen planos cercanos que muestren rasgos reconocibles y evite que terceros no autorizados accedan a los controles de la cámara.
5. Si se emplean cámaras **de video conectadas a Internet que permiten un acceso remoto a**

través de la Red al visionado de las imágenes en tiempo real para el control de la actividad de los trabajadores, deben ser informados y respetarse sus derechos. Si se van a difundir imágenes de una empresa con fines promocionales es necesario obtener el consentimiento de los empleados.

6. Asegúrese de que si los menores utilizan webcams para realizar videollamadas, chat con video o mostrar imágenes en tiempo real a amistades, lo hacen de forma segura y controlada y compruebe que los menores realizan un uso apropiado, bajo su supervisión de las webcam.

Asimismo, se incluye como recomendación a los fabricantes y distribuidores de estos dispositivos que faciliten, junto con la documentación o instrucciones, **el Decálogo para usuarios de videocámaras conectadas a Internet.**

El informe completo se puede consultar en

https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/plan_sectorial_camaras_internet_2009.pdf