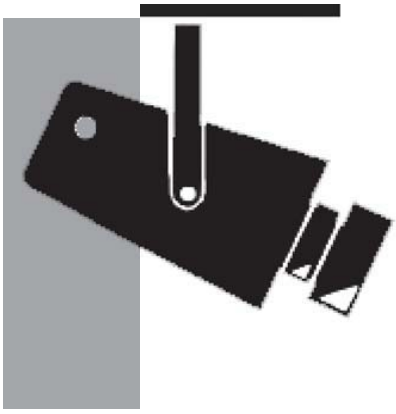
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



Inspección Sectorial de Oficio

Videocámaras en Internet.

Agencia Española de Protección de Datos

Junio de 2009

ÍNDICE

► Inspección sectorial de oficio:

Videocámaras en Internet.

1. OBJETO Y ALCANCE

El presente plan tiene por objeto elaborar recomendaciones y establecer pautas que permitan el empleo de este tipo de dispositivos dentro del marco de la normativa de protección de datos.

Con el fin de lograr este objetivo, se ha efectuado un análisis de las situaciones más habituales detectadas en la Red, sin entrar a realizar un estudio estadístico sobre su frecuencia que, aunque sin duda interesante, no modificaría en absoluto las conclusiones del presente estudio.

A los efectos del presente informe se entiende por **cámaras IP**[1] a las cámaras de vídeo conectadas a Internet que permiten un acceso remoto a través de la Red al visionado de las imágenes en tiempo real.

Se entiende también que dicho acceso se realiza utilizando simplemente un navegador, sin que sea necesario el empleo de ningún programa o herramienta de intrusión (*hacking).*

2. ANTECEDENTES

El uso cámaras de vídeo se ha extendido[2] de forma generalizada en los últimos años. A medida que la tecnología se ha desarrollado su coste ha disminuido progresivamente hasta convertirse en dispositivos al alcance del gran público.

[1] La denominación de "cámara IP" viene del hecho de que incorporan la tecnología IP base de la red Internet y de otras redes públicas. Por IP se entiende un conjunto de protocolos que permiten la comunicación entre dos dispositivos IP a través de una red IP como es Internet.

[2] Según un estudio al que ha tenido acceso esta Agencia, los crecimientos de ventas en cámaras IP a nivel europeo se han situado por encima del 40% en los años precedentes, habiéndose revisado esas expectativas hacia el 30% para los próximos años como consecuencia de la actual crisis. La cuota de penetración de las cámaras IP es del 23% de media en Europa, siendo del 20% en España. Eso significa que aún 8 cámaras de cada 10 que se venden son analógicas aunque la tendencia es que las digitales ganen mercado en detrimento de las analógicas.

Según este estudio, el fabricante Axis es el primer suministrador de cámaras IP del mundo con un 33,5% de cuota de mercado, siendo del 40% en Europa y de casi un 48% en España. Respecto a las cámaras en total incluyendo las analógicas, Axis figura como tercer suministrador mundial de cámaras por detrás de Panasonic y Pelco y por delante de Bosch. En Europa la primera posición es de Bosch seguida de Axis y Panasonic.

La incorporación de la tecnología IP ha incrementado las posibilidades de interconexión. De cámaras pensadas inicialmente para formar partes de circuitos cerrados de televisión muy localizados (los denominados CCTV) se ha pasado a las cámaras IP capaces de conectarse directamente a redes públicas con alcance global, sin que se requiera para ello de un ordenador como equipo intermedio entre la cámara y la Red.

La tecnología IP ha permitido también incluir en una única conexión todas las funcionalidades disponibles de la cámara: vídeo, sonido, control de movimiento, zoom, etc, facilitando así su instalación que responde a la filosofía *"plug & play",* o de conectar y funcionar.

Adicionalmente, la evolución tecnológica ha permitido disminuir su tamaño de forma considerable hasta el punto que su presencia puede pasar inadvertida incluso para aquellos cuya imagen esté siendo captada.

Esta mayor flexibilidad en cuanto a interconexión, funciones y alcance geográfico ha llevado también a la aparición de nuevas finalidades y usos. Inicialmente utilizados con fines básicamente de seguridad, en cuanto a protección de bienes y personas, han surgido otros como los relativos al control de la actividad laboral y el de difundir la actividad de un determinado espacio, ya sea abierto o cerrado, público o privado. A modo de ejemplo podría citarse la webcam que recoge información de tráfico de una autopista o la que difunde la actividad en el interior de una empresa.

Además de estos usos generales, también pueden producirse otros más específicos como son, por ejemplo, los relativos al estudio de hábitos de comportamiento fundamentalmente asociados al consumo y que pueden darse en superficies comerciales, etc. En este sentido, puede producirse en la práctica la confluencia de distintas finalidades de las ya citadas sobre una misma instalación.

Esta evolución ha ido en paralelo a la implantación y difusión de la normativa de protección de datos. Desde la primera Ley de 1992 conocida como LORTAD sustituida en 1999 por la actual LOPD, la sociedad española ha ido tomando una mayor conciencia de su privacidad. A ello ha contribuido sin duda la labor de esta Agencia desde su constitución en 1993.

En esta mirada retrospectiva hay que remontarse hasta el año 2000 para encontrar el primer caso en el que la utilización de cámaras conectadas a Internet topa con la privacidad. Se trataba de una denuncia contra un diario deportivo formulada por una empleada del mismo. La dirección del periódico había decidido instalar una *WebCam* en su redacción y difundir las imágenes en tiempo real a través de Internet con objeto de acercar la redacción a sus lectores. La Agencia resolvió este caso sancionando al periódico por una infracción grave al proceder al tratamiento de las imágenes de sus trabajadores con la finalidad citada sin acreditar el correspondiente consentimiento informado para ello.

En la resolución, la Agencia consideró que la imagen de una persona es un dato de carácter personal sujeto al ámbito de aplicación de la LOPD. Ello tenía su fundamento en el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, en el que se considera dato de carácter personal a: *"toda*

información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"..

También se tuvo en cuenta en aquel momento la doctrina del Tribunal Constitucional, que en su sentencia 292/2000 extendía el ámbito de cobertura de la protección de datos no solo a los datos íntimos sino a cualquier tipo de dato personal sea íntimo o no.

Con estos fundamentos la Agencia sentaba un criterio que ha venido siendo confirmado posteriormente. En este sentido conviene citar la sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003, conocida como *sentencia Lindqvist*[3] y de la que se desprende que la difusión en Internet de referencias a personas identificadas constituiría un tratamiento de datos personales amparado dentro del ámbito de aplicación de la Directiva 95/46 sobre protección de datos de carácter personal.

De forma adicional, del Dictamen 4/2007 sobre el concepto de *dato personal* elaborado por el Grupo de Trabajo[4] del artículo 29 de la Directiva 95/4 y del que esta Agencia forma parte activa, se desprende que las imágenes de personas obtenidas por medio de cámaras de vídeo pueden considerarse datos personales en la medida en que estas personas sean reconocibles.

Finalmente, el Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2008, considera dato de carácter personal la información gráfica, fotográfica y de vídeo.

Así pues, la captación de imágenes de personas que permitan su reconocimiento y su difusión en Internet constituye un tratamiento de datos de carácter personal sometido a la LOPD. No obstante, cabe puntualizar que no siempre se hace preciso recabar el consentimiento de los afectados para dicho tratamiento.

En efecto, el artículo 6.1 de la LOPD establece que *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".* A esta excepción pueden acogerse dos finalidades en la práctica muy habituales y respecto de las cuales existen respectivamente normas con rango de Ley que eximirían de recabar dicho consentimiento en determinadas condiciones. Estas

[3] Sentencia del Tribunal de Justicia de la Unión Europea (asunto. C-101/01, de 6 de noviembre de 2003, sentencia Lindqvist) cuyo fallo primero establece que "*La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos".*

[4] Conocido como Grupo del Artículo 29 por estar constituido al amparo de dicho artículo de la Directiva 95/46. Forman parte del grupo de trabajo todas la Agencias nacionales europeas de protección de datos. Entre sus funciones se encuentran las de elaborar dictámenes y recomendaciones sobre los asuntos relacionados con la protección de datos personales en la Comunidad Europea, así como contribuir a la armonización de los criterios aplicados por las diferentes agencias.

finalidades son la captación de imágenes para el **control de la actividad laboral** y para la **seguridad de bienes y personas o videovigilancia**.

En el caso del **control de la actividad laboral**, el amparo viene dado en el Estatuto de los Trabajadores (Real Decreto Legislativo 1/1995) que faculta al empresario para implantar sistemas de vigilancia y control sin que sea necesario el consentimiento de los trabajadores y siempre que no se atente contra su dignidad.

Esta facultad otorgada al empresario no es absoluta y ha sido limitada por la doctrina emanada del Tribunal Constitucional. Así, en su sentencia **STC 98/2000** y respecto de la monitorización en el lugar de trabajo mediante grabaciones de vídeo y audio, se establece la necesidad de preservar un necesario equilibrio entre el interés empresarial del control de la actividad laboral y la libertad constitucional de los trabajadores. Dicho equilibrio pasa por la aplicación del principio de proporcionalidad y de intervención mínima.

El criterio para evaluar la proporcionalidad de una medida restrictiva de derechos fundamentales se encuentra claramente detallado en la sentencia **STC 186/2000** del citado Tribunal. Según este criterio, la medida es proporcional si se cumplen los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad y de intervención mínima); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Estos criterios establecidos a nivel nacional se refuerzan con los recogidos a nivel europeo. Así, el **Dictamen 8/2001** sobre el tratamiento de datos en el entorno laboral del Grupo de Trabajo del artículo 29 de la Directiva 95/46, establece que los principios de protección de datos aplican a la monitorización y vigilancia de los trabajadores y en especial al uso del correo electrónico, el acceso a Internet, los datos de localización y los sistemas de videocámaras. Establece, además, el principio de proporcionalidad en el empleo de los mecanismos de monitorización y el principio de calidad en cuanto a que los datos personales tratados deberán ser adecuados, pertinentes y no excesivos para la finalidad para la cual la monitorización está justificada. Adicionalmente se establecen también los principios de información y transparencia, acceso, retención y confidencialidad y seguridad de los datos. En el mismo sentido se pronuncia el **Dictamen 4/2004** sobre tratamiento de datos personales mediante sistemas de videocámaras, elaborado por el mismo grupo de trabajo.

En resumen, el artículo 20.3 de Estatuto de los Trabajadores facultaría al empresario al tratamiento de imágenes de sus trabajadores con fines de vigilancia y control cuando dicha medida resulte equilibrada con los derechos fundamentales de trabajador y en especial con su derecho a la intimidad y siempre y cuando se ajuste también al principio de proporcionalidad.

Si bien bajo estos supuestos dicho tratamiento quedaría legitimado sin necesidad del consentimiento de los trabajadores, ello sería sin perjuicio del

resto de principios y obligaciones recogidos en la LOPD, entre los que se encuentran los principios de información, calidad, seguridad y deber de secreto, notificación del fichero, cancelación de las imágenes así como los derechos de los afectados en cuanto a acceso, rectificación, cancelación y oposición.

En el caso de la **seguridad de bienes y personas o videovigilancia**, el amparo vendría dado en la Ley Orgánica 4/1997[5], para las imágenes captadas por la Fuerzas y Cuerpos de Seguridad en lugares públicos y privados.

Si bien no han sido incluidas en el presente plan las imágenes captadas por la Fuerzas y Cuerpos de Seguridad, conviene resaltar que, de acuerdo a dicha Ley, la captación de imágenes de la vía pública que incluyan personas identificadas o identificables se encuentra reservada con carácter exclusivo a las Fuerzas y Cuerpos de Seguridad con fines de videovigilancia. Se excepcionan de este principio general las imágenes captadas por particulares dentro de un ámbito estrictamente privado o doméstico.

En el caso de que las imágenes fueran captadas por entidades públicas o privadas y fuera de la vía pública, con fines de seguridad, el amparo vendría dado por la **Ley 23/1992**, de 30 de julio, de **Seguridad Privada** donde se recoge una legitimación siempre que se cumpla lo previsto en la citada Ley y, de forma adicional, lo establecido en la LOPD.

Al igual que en el supuesto de control de la actividad laboral, también resulta aplicable aquí la doctrina constitucional basada en el principio de proporcionalidad e intervención mínima, así como los dictámenes elaborados en el grupo de trabajo del artículo 29 de la Directiva 95/46.

Con objeto de unificar lo expuesto hasta ahora, incluyendo la citada doctrina, esta Agencia dictó la **Instrucción 1/2006**, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras. Posteriormente, en 2007, público la ***Guía sobre videovigilancia*** que recoge, de forma clara, diferentes casuísticas y las pautas a seguir en cada una de ellas.

Llegado a este punto, y teniendo en cuenta la fuerte expansión que están tenido las cámaras IP, el marco legal descrito, y el potencial impacto que para la privacidad presentan estos dispositivos, esta Agencia ha considerado conveniente complementar la Instrucción 1/2006 y la Guía sobre videovigilancia mediante la realización de un plan de oficio específico para dichos dispositivos.

Consecuencia del creciente impacto para la privacidad es el incremento experimentado en el número de denuncias y consultas recibidas así como en la mayor sensibilidad social de la que se han hecho eco los medios de comunicación generándose debate público[6] incluso en Internet.

[5] Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de las videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

[6] Cabe señalar, a título de ejemplo, la difusión de imágenes a través de Internet de una zona de Madrid realizada por varios vecinos al objeto de eliminar la prostitución existente

Recientemente, se ha publicado también un estudio realizado por la Asociación de Internautas en el que se concluye que el 80 % de cámaras IP instaladas presenta riesgos potenciales para la privacidad en la medida en que carecen del adecuado control de acceso[7].

En definitiva, el presente plan tiene por objeto analizar los usos más habituales de las cámaras IP y su encaje jurídico, ofreciendo pautas de actuación de manera preventiva tendente a evitar una acción sancionadora posterior.

3. DESCRIPCIÓN DEL FUNCIONAMIENTO

Existen en el mercado multitud de cámaras IP de diferentes fabricantes y modelos:

en dicha zona. Esta situación tuvo un amplio eco en los medios de comunicación y dio lugar a la apertura de actuaciones por parte de la Agencia.

[7] En el citado informe se afirma que el 60% de las cámaras conectadas a Internet carece de control de acceso mientras que del 40% restante que sí presenta algún tipo de control de acceso, éste es deficiente en la mitad de ellas. En definitiva, el 80 % de cámaras IP instaladas presenta riesgos potenciales para la privacidad en la medida en que carecen del adecuado control de acceso.
Sin poner en duda la veracidad de estos datos arrojados en el informe, lo cierto es que dentro del 60% de cámaras sin control de acceso detectadas se han incluido también las que recogen imágenes de paisajes o panorámicas, en las que no sería exigible controles de accesos al no resultar identificables las personas físicas.
Si bien es difícil precisar la cuantía de cámaras que ofrecen imágenes panorámicas y su contabilización excede del presente estudio, lo cierto es que dicho porcentaje se reduciría considerablemente dado que muchas de las cámaras instaladas son de este tipo. Esta consideración no resta importancia a la problemática suscitada dado el volumen cada vez mayor de cámaras que sí recogen imágenes de personas y el fuerte impacto que representan para la privacidad.

A diferencia de las cámaras tradicionales de circuito cerrado de TV, donde la cámara ha de conectarse directamente al monitor por un cable de vídeo, las denominadas “cámaras IP” permiten que la imagen captada por ésta sea visualizada en un ordenador remoto siempre que cámara y ordenador se encuentren conectados a la misma red IP como es el caso de Internet.

En este sentido la cámara IP puede conectarse a la red Internet directamente como si fuera un ordenador más, por lo que, como cualquier dispositivo conectado a la red, ha de disponer de una dirección IP que la referencia de forma univoca dentro de la Red.

De hecho, a un punto de acceso a Internet determinado puede conectarse una única cámara o un conjunto de cámaras tal y como se representa en la figura adjunta:

La visualización de las imágenes captadas por la cámara puede realizarse desde cualquier ordenador conectado a Internet a través del navegador habitual, sin más que invocar la dirección IP de la cámara y siempre que no se hayan establecido controles de acceso a la misma.

Desde el mismo ordenador también es posible acceder al resto de funcionalidades disponibles en la cámara: zoom, movimiento horizontal, movimiento vertical, sonido, etc., así como grabar las imágenes recibidas.

Por lo general, las cámaras suelen disponer de mecanismos de control de acceso basados en usuario y clave de forma que, si este control se encuentra activado en la cámara, cualquier ordenador que invoque su dirección IP deberá pasar dicho control antes de poder acceder a los servicios ofrecidos por la cámara incluidas las imágenes.

Es habitual también que los mecanismos de control de accesos vengan desactivados de fábrica o bien activados con usuarios y claves por defecto[8], resultando una práctica habitual que se instalen tal y como vienen de fábrica.

Lo anterior hace que la cámara IP sea vulnerable, ya que deja a la cámara en una situación de “puertas abiertas”, sin más protección frente al acceso indebido de un tercero que conocer donde su localización en la Red, es decir, su dirección IP.

Esta situación, que en si misma pudiera considerarse de riesgo limitado dado el tamaño de la Red, resulta en la práctica de un riesgo elevado como consecuencia de los buscadores. Éstos últimos como Google, Yahoo, etc. disponen de robots que rastrean permanentemente la Red generando una base de datos de contenidos en la Red, a la vez que proporcionan mecanismos de búsqueda muy efectivos sobre dichos contenidos, permitiendo localizar direcciones IP correspondientes a cámaras.

El mecanismo de localización a través de un buscador sería el siguiente:

- Cada fabricante o modelo de cámara conectada a Internet emite lo que se denomina un mensaje de presentación cuando su dirección IP es invocada desde un ordenador conectado a Internet.

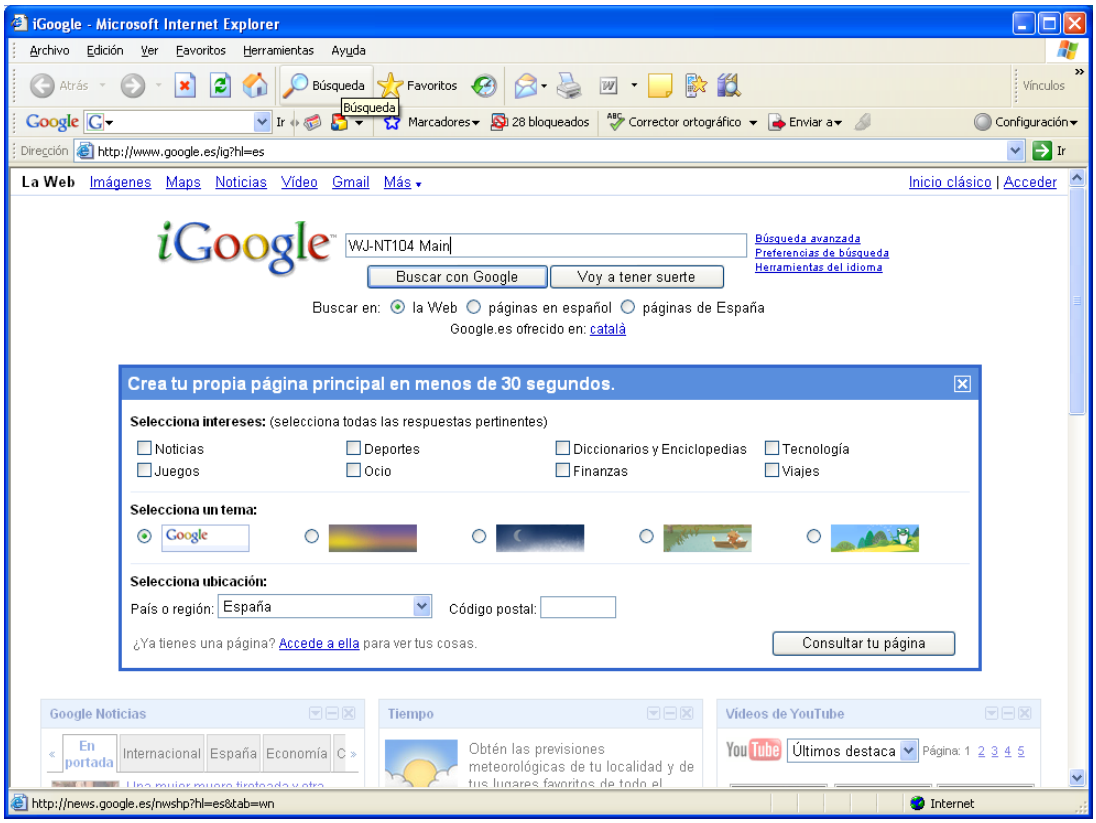
  El acceso a los mensajes de presentación puede obtenerse fácilmente realizando con el buscador una solicitud de información sobre cámaras en Internet.

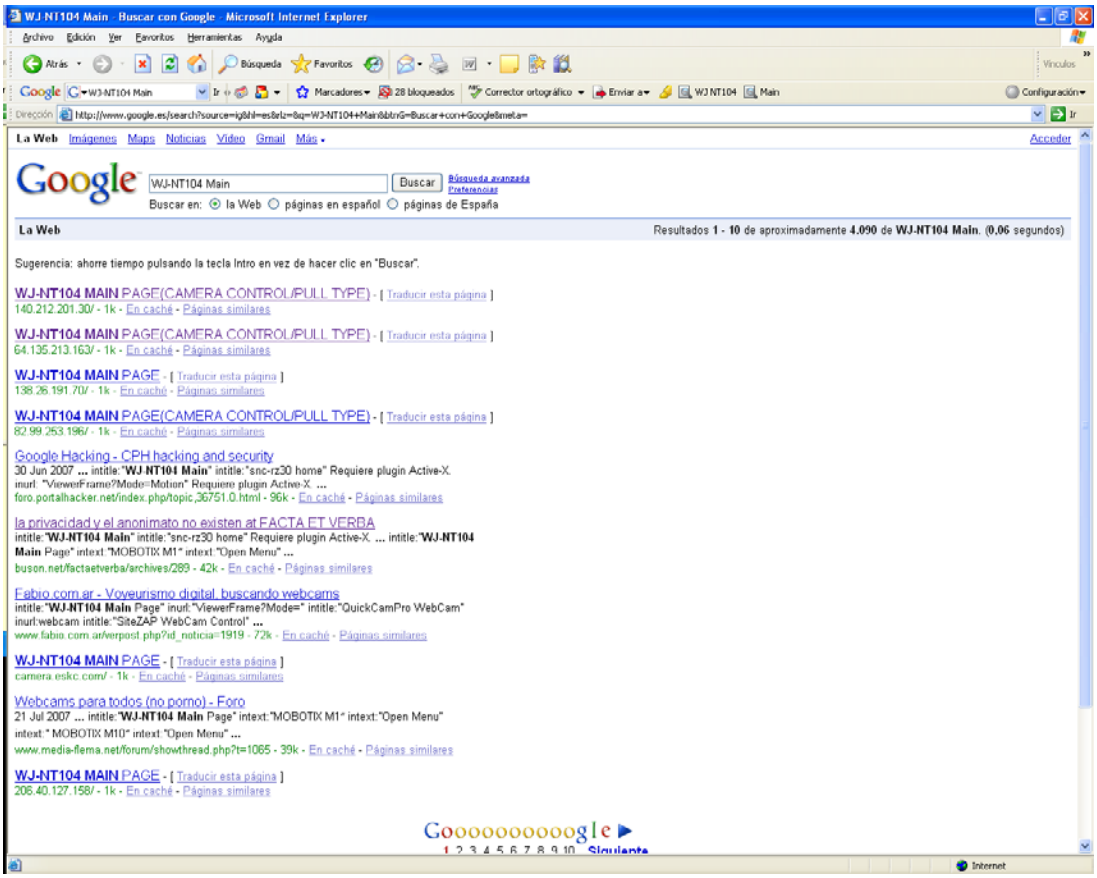
  Con esta búsqueda se obtienen relaciones con mensajes de presentación de conocidas marcas de videocámara como son, entre otras, Axis, Canon, Mobotix, JVC, Flex Watch, Panasonic, Toshiba, Sony.

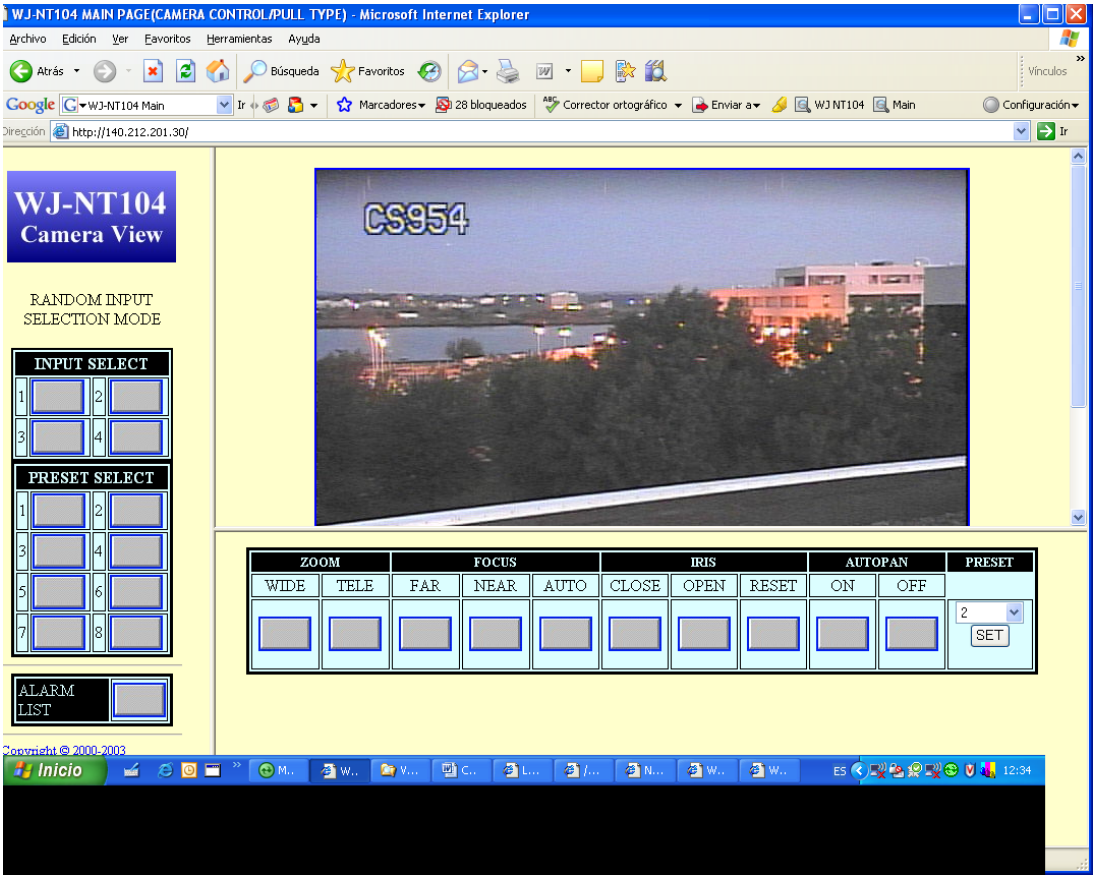
- Los buscadores que rastrean la red de forma sistemática cuando invocan una dirección IP correspondiente a una cámara reciben su mensaje de bienvenida indexando en sus bases de datos la dirección IP asociada al mensaje de bienvenida.
- Esto permite que cuando un usuario interrogue a un buscador por un mensaje de bienvenida concreto le aparezcan multitud de referencias o enlaces a las direcciones IP donde se encuentran conectadas dichas cámaras.
- A continuación, con una simple selección por parte del usuario de un enlace de los ofrecidos por el buscador el usuario va a conseguir conectarse a la cámara si esta no dispone de control de acceso o dicho control es deficiente (usuario y contraseña por defecto). Las imágenes recogidas a continuación reflejan la búsqueda a través de

[8] Las cámaras que disponen de la posibilidad de establecer un usuario y contraseña suelen venir de fábrica con dicho mecanismo desactivado, es decir sin control de acceso alguno, o con un usuario y contraseña prefijados e iguales para todas cámaras del mismo modelo y/o fabricante. A este usuario y contraseña asignados por el fabricante se denomina usuario y contraseña por defecto.

GOOGLE de una videocámara en Internet, la respuesta obtenida del buscador y finalmente una de las cámaras accedidas tras seleccionar la primera de las respuestas ofrecida por el buscador.




WJ-NT104 Main - Buscar con Google - Microsoft Internet Explorer
Google
WJ-NT104 Main
Buscar
La Web
Resultados 1 - 10 de aproximadamente 4.090 de WJ-NT104 Main. (0,06 segundos)
WJ-NT104 MAIN PAGE(CAMERA CONTROL/PULL TYPE)
WJ-NT104 MAIN PAGE
Google Hacking - CPH hacking and security
la privacidad y el anonimato no existen at FACTA ET VERBA
Fabio com ar - Voyeurismo digital, buscando webcams
Webcams para todos (no porno) - Foro


WJ-NT104 MAIN PAGE(CAMERA CONTROL/PULL TYPE) - Microsoft Internet Explorer
WJ-NT104
Camera View
RANDOM INPUT
SELECTION MODE
INPUT SELECT
PRESET SELECT
ALARM
LIST
CS954
ZOOM
FOCUS
IRIS
AUTOPAN
PRESET
WIDE
TELE
FAR
NEAR
AUTO
CLOSE
OPEN
RESET
ON
OFF
SET
Copyright © 2000-2003
Inicio

4. MARCO LEGAL

La normativa legal aplicable a esta actividad es la siguiente:

- Constitución Española; Art. 18.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)
- Real Decreto 1332/1994, de 20 de junio, que desarrolla determinados aspectos de la Ley Orgánica 5/1992. (en vigor de conformidad con lo dispuesto en la disposición Transitoria Tercera de la Ley Orgánica 15/1999)
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- Ley Orgánica 4/1997, de 4 agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, (LO 4/1997).
- Real Decreto 596/99, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen (LO 1/1982).
- Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la Seguridad Ciudadana, (LO 1/1992).), modificada por la Ley 10/1999 de 21 de abril.
- Ley 23/1992, de 30 de julio, de Seguridad Privada.
- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.
- Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido del Estatuto de los Trabajadores.

De la normativa anterior se deduce lo siguiente:

La captación de imágenes con cámaras y su difusión a través de Internet está sujeta a la Ley Orgánica 15/1999, de 13 de diciembre de protección de los datos de carácter personal en la medida en que dichas imágenes afecten a personas identificadas o identificables.

La LOPD define dato de carácter personal como cualquier información concerniente a personas físicas identificadas o identificables. En este sentido su Reglamento de Desarrollo[9] recoge que la información gráfica y

[9] El Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2008, de 20 de junio, define en su artículo 5.1. apartado f) dato de carácter personal como "*cualquier*

fotográfica de una persona se considera dato de carácter personal en la medida que permita su identificación. Así pues, las imágenes de personas que permitan su reconocimiento se consideran un dato de carácter personal y quedan por lo tanto, dentro del ámbito de aplicación de la LOPD.

El tratamiento de imágenes comprende la captación, grabación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas. De esta manera, se considera tratamiento de datos personales la difusión de las citadas imágenes a través de Internet.

Se excepcionan del ámbito de aplicación de la LOPD las imágenes captadas para uso o finalidad doméstica de conformidad con lo establecido en el artículo 2 a) de la LOPD. Se entiende por finalidad doméstica el tratamiento realizado por una persona física en el marco de una actividad exclusivamente privada o familiar, por lo que no puede considerarse finalidad doméstica la difusión de imágenes de terceros a través de Internet en abierto.

Para la captación de imágenes de acuerdo a lo previsto en la LOPD será de aplicación los principios de **legitimación** o consentimiento, de **información**, de **seguridad** y el **deber de secreto**.

4.1. PRINCIPIO DE LEGITIMACIÓN.

Establece las condiciones que legitiman la capacidad de tratar datos de terceros. La norma general[10] consiste en recabar el consentimiento de los afectados, no obstante, se puede obtener también la legitimación cuando

información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". El apartado o) establece que se considerará identificable a "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".*

[10] El artículo 6 de la LOPD establece que *"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado."*

exista una previsión legal o cuando el tratamiento de los datos se realice en el marco de una relación jurídica.

4.2. PRINCIPIO DE INFORMACIÓN.

Establece la información que se debe de facilitar a los afectados respecto de los cuales se pretenda tratar sus datos. En este sentido, la LOPD provee[11] que se informe a los afectados de forma previa a la recogida de sus datos personales de la existencia de un fichero o tratamiento, su finalidad y de quienes van a ser los destinatarios de la información, así como de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición por parte del afectado.

Dado el especial impacto que para la privacidad presenta la instalación de cámaras se ha considerado oportuno diseñar procedimientos específicos para informar *in-situ* a las personas cuyas imágenes puedan ser captadas por estos sistemas. En este sentido, la Instrucción 1/2006 incorpora un distintivo informativo cuyo uso y exhibición es obligatoria[12]:

[11] El artículo 5 de la LOPD establece: *"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante."*

[12] El cartel se encuentra también accesible en: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/normativa_estatal/index-ides-idphp.php#video)

Este distintivo se ubicará como mínimo en los accesos a las zonas vigiladas, sean estos exteriores o interiores. Debe tenerse en cuenta que si el lugar vigilado dispone de varios accesos se debe colocar en todos ellos al objeto de que la información sea visible con independencia de por donde se acceda

Adicionalmente a los distintivos, se habilitarán impresos que contendrán toda la información a la que se refiere el artículo 5 de la LOPD[13]

4.3. PRINCIPIO DE SEGURIDAD.

Establece las medidas técnicas y organizativas que el responsable del tratamiento debe de implantar al objeto de garantizar la seguridad e impedir que terceros no autorizados accedan a los datos. Esta política de seguridad[14] se encuentra desarrollada en el Título VIII del Reglamento de Desarrollo de la LOPD (aprobado por RD 1720/2007).

En el caso de imágenes captadas con fines de control laboral o de vigilancia de bienes y personas o videovigilancia y sin perjuicio de cumplir con los principios de legitimación e información, deberá de garantizarse el principio de seguridad. De acuerdo a este principio, sólo aquellas personas encargadas de llevar a cabo las funciones de vigilancia y control deberán de

[13] Dicho impreso deberá informar al menos sobre:

- La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

El impreso deberá estar disponible existiendo cuando menos la posibilidad de imprimirlo a petición del afectado. La información del impreso podrá incorporarse al cartel anunciador y sustituirlo únicamente en aquellos casos en los que por su contenido y por la ubicación del mismo la información resulte legible e inteligible. (a modo de ejemplo, si el cartel se encuentra situado en puertas o lugares de acceso y ubicado dentro del campo de visión natural del afectado, esto es a la altura de sus ojos.)
El uso de la señal y el impreso, no excluye la existencia de métodos adicionales de información que se añadan a los dos anteriores como publicación en web de políticas de privacidad, información a la representación sindical si la hubiere etc.

[14] La LOPD en su artículo 9 establece *"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."*

disponer de acceso a las imágenes captadas, por lo que éstas no podrán ser difundidas en abierto a través de Internet.

Deberá, por lo tanto, habilitarse un mecanismo de control que garantice que únicamente disponen de acceso a las imágenes las personas encargadas de las funciones de vigilancia y control. De lo contrario se vulneraría el principio de seguridad.

Es aconsejable consultar la Guía de Seguridad de Datos disponible en el Canal de Documentación del website de la Agencia:

https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/index-ides-idphp.php

4.4. PRINCIPIO DE DEBER DE SECRETO.

Establece la obligación[15] para todas aquellas personas que intervengan en el tratamiento de mantener el secreto profesional respecto de los datos personales a los que tienen acceso como consecuencia de sus funciones.

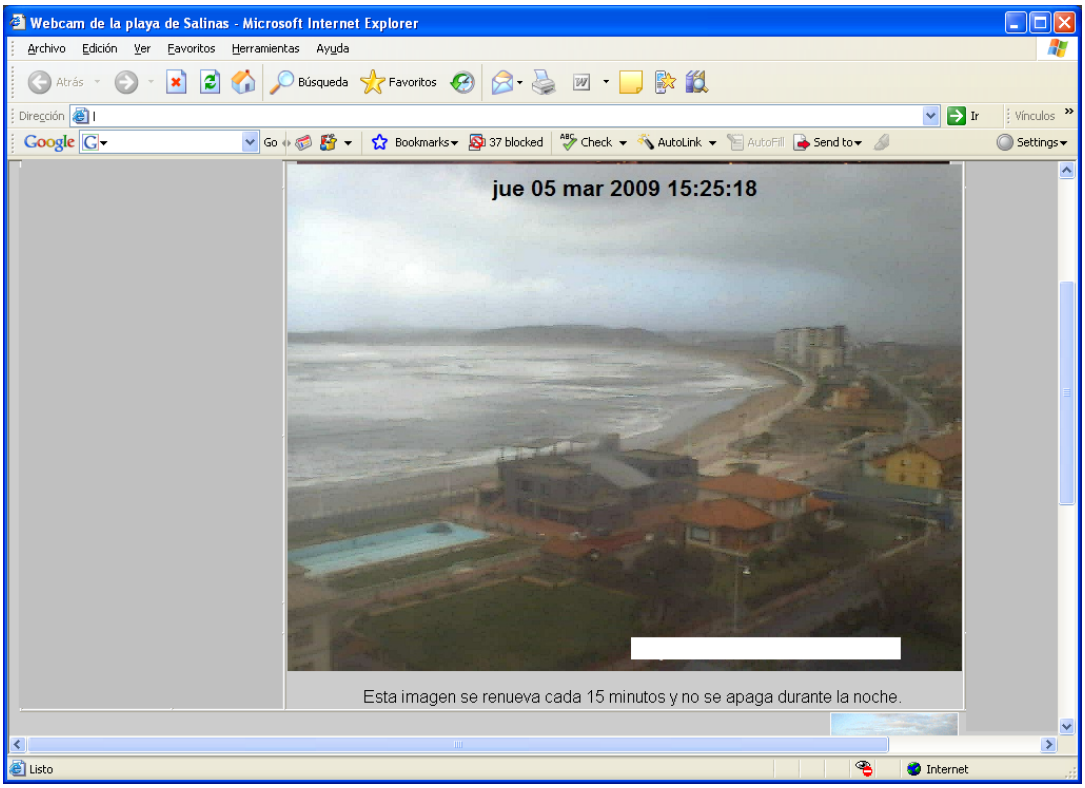
A continuación se detallan las situaciones más típicas detectadas y su impacto para la privacidad desde la óptica de los cuatro principios mencionados.

[15] El artículo 10 de la LOPD establece que *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

5. TIPOLOGÍAS DE WEB ANALIZADAS

5.1. CAPTACIÓN DE IMÁGENES DE PAISAJES O PANORÁMICAS.

A modo de ejemplo ilustrativo se ha anexado la siguiente imagen:



La captación de imágenes de paisajes o panorámicas, en la medida en que no permitan identificar a las personas cuya imagen pueda ser captada quedaría fuera del ámbito de aplicación de la normativa de protección de datos y no existiría transgresión de ninguno de los principios aludidos por lo que, sin perjuicio de otra normativa que pudiera ser de aplicación en cada caso concreto, no habría ninguna limitación y dicha difusión podría realizarse en abierto, es decir, sin necesidad de activar ningún tipo de control de acceso a las imágenes captadas por la cámara.

5.2. CAPTACIÓN DE IMÁGENES DE LA VÍA PÚBLICA

A modo de ejemplo ilustrativo se ha anexado la siguiente imagen:

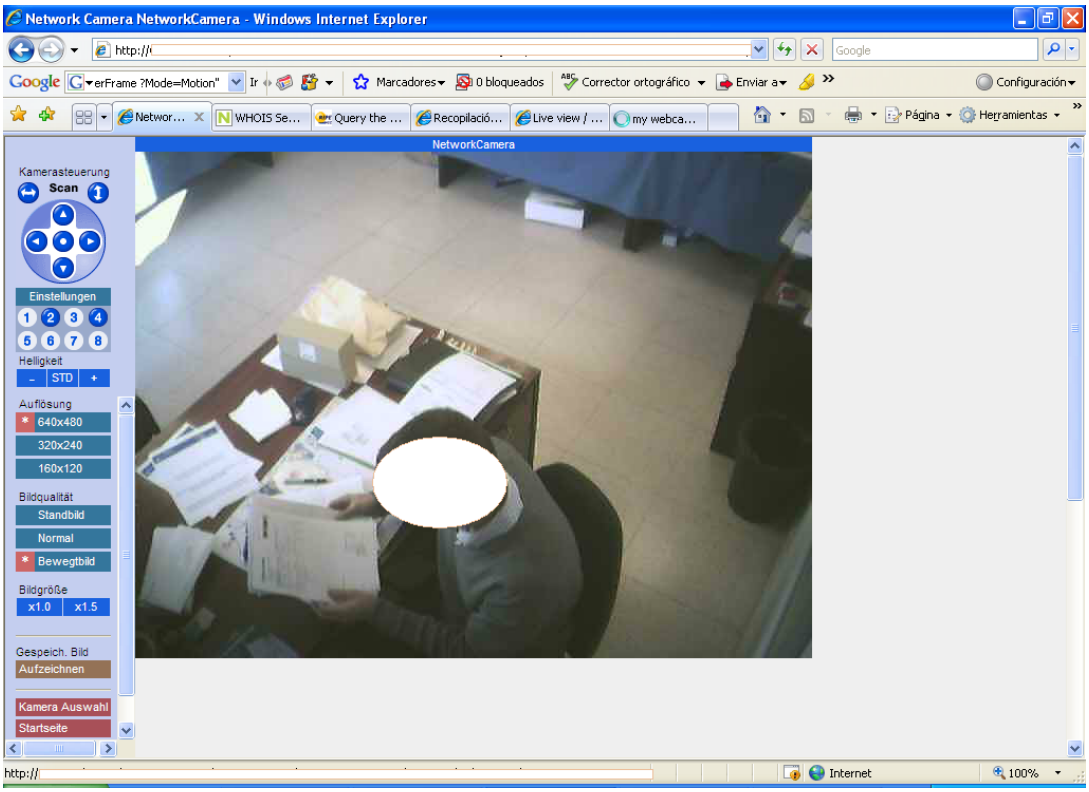
La captación de imágenes de la vía pública de personas identificadas o identificables y fuera de un ámbito estrictamente privado o domestico se encuentra reservada, con carácter exclusivo, a las Fuerzas y Cuerpos de Seguridad del Estado con fines de videovigilancia, en consonancia con lo establecido en la Ley Orgánica 4/1997.

Resulta por lo tanto contrario a la normativa de protección de datos, salvo la excepción citada, la captación y difusión de imágenes de la vía pública en las que pueda identificarse a las personas.

La captación y difusión de imágenes de este tipo a través de Internet excedería con mucho el ámbito privado o doméstico por lo que se produciría una vulneración del **principio de legitimación**.

5.3. CAPTACIÓN DE IMÁGENES EN EL LUGAR DE TRABAJO.

A modo de ejemplo ilustrativo se han anexado las siguientes imágenes:



Respecto del principio de legitimación y como ya se ha indicado, el artículo 6 de la LOPD legítima el tratamiento cuando se recaba el consentimiento de los afectados o una Ley autoriza el mismo. Entre las excepciones previstas a esta norma general se encuentra la que establece que no es necesario dicho consentimiento cuanto el tratamiento sea necesario para el adecuado desenvolvimiento de la relación laboral de los trabajadores con la empresa.

Como ya se ha señalado en el apartado de antecedentes, el Estatuto de los Trabajadores (ET) faculta[16], con ciertas salvaguardas, al empresario para implantar sistemas de control de la actividad laboral sin que precise para ello del consentimiento de los trabajadores.

No obstante, atendiendo a la doctrina constitucional existente, dicha facultad no es absoluta y se encuentra sujeta al principio de proporcionalidad e intervención mínima, por lo que debe modularse a tenor los derechos constitucionales que asisten al trabajador.

En este contexto, la difusión de imágenes a través de Internet en abierto, atentaría contra el principio de proporcionalidad así como contra los principios de seguridad o secreto, al permitir que terceros ajenos dispongan de acceso a las imágenes.

Así pues, el empresario estaría legitimado para tratar datos de sus empleados con fines de control laboral sin contar con el consentimiento previo de los empleados siempre que la medida sea proporcional, el trabajador haya sido debidamente informado de ella y se respeten los principios de seguridad y secreto. Obviamente, los datos recabados bajo este supuesto no podrán ser utilizados para fines distintos[17].

Dicho tratamiento, aunque legítimo, quedaría plenamente sometido a la LOPD, debiéndose de cumplir con los siguientes requisitos específicos[18]:

- Se respetará de modo riguroso el principio de proporcionalidad:
  - Se adoptará esta medida cuando no exista otra más idónea.
  - Las instalaciones, en caso de utilizarse, se limitarán a los usos estrictamente necesarios captando imágenes en los espacios indispensables para satisfacer las finalidades de control laboral.
  - No podrán utilizarse estos medios para fines distintos de los propios del control laboral salvo que se trate de fines legítimos y se adopten las medidas pertinentes para el cumplimiento de la normativa que les sea de aplicación.
- Tendrán en cuenta los derechos específicos de los trabajadores respetando:

[16] El Estatuto de los Trabajadores (ET) en su artículo 20.3 dispone que *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".*

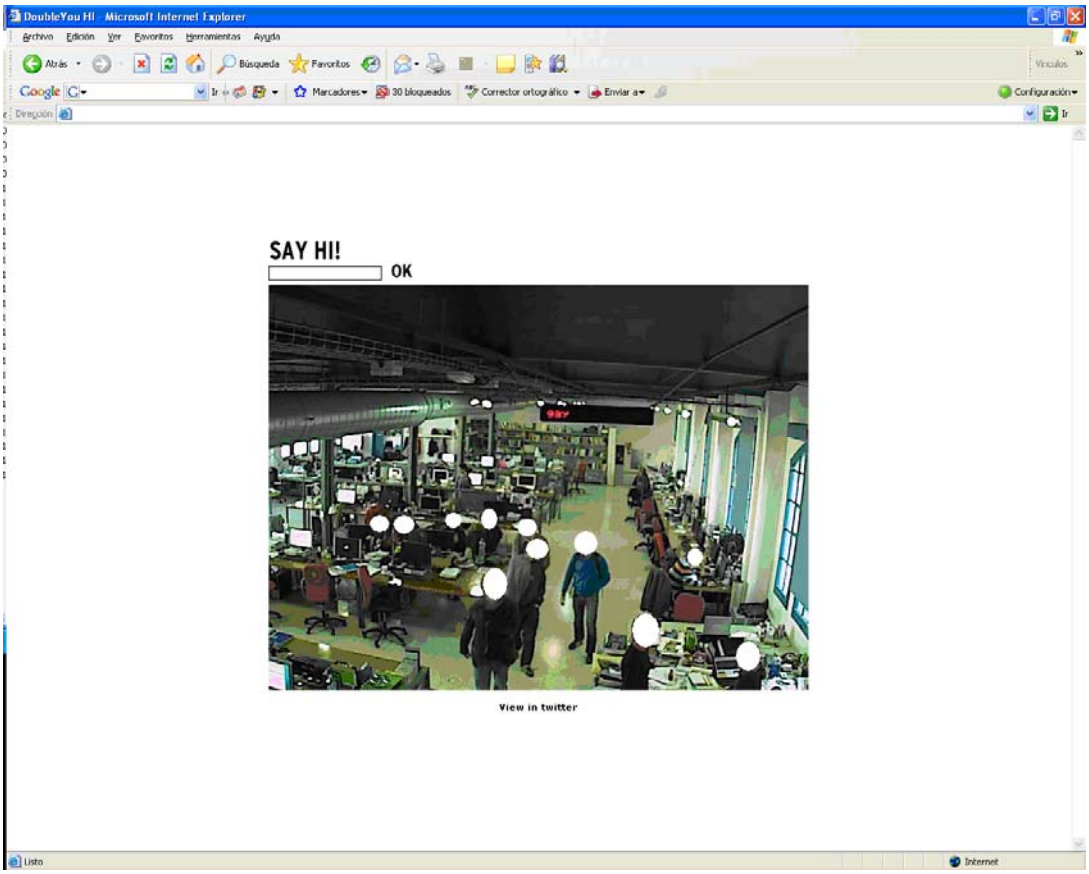
[17] El artículo 4 de la LOPD establece que: *"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".*

[18] Se recomienda consultar la guía de videovigilancia disponible en la website de la Agencia (www.agpd.es)

- Los derechos a la intimidad y el derecho fundamental a la protección de datos en relación con espacios vetados a la utilización de este tipo de medios como vestuarios, baños, taquillas o zonas de descanso.
- El derecho a la propia imagen de los trabajadores.
- La vida privada en el entorno laboral no registrando en particular las conversaciones privadas.

- Se procederá a la creación e inscripción del correspondiente fichero si existe grabación de las imágenes.
- Se garantizará la cancelación de las imágenes en el plazo máximo de 30 días y únicamente podrán conservarse aquellas que registren una infracción o incumplimiento de los deberes laborales.
- Se garantizarán los derechos de acceso y cancelación.
- Se formalizarán en su caso contratos de acceso a los datos por cuenta de terceros.

Se han detectado casos en los que la difusión de imágenes de un centro de trabajo no obedece a una finalidad de control laboral sino de ofrecer una imagen empresarial o de negocio, dando a conocer una organización a sus clientes y potenciales clientes mediante la difusión de la actividad en sus instalaciones incluyendo a empleados, como por ejemplo el caso de la imagen adjunta:



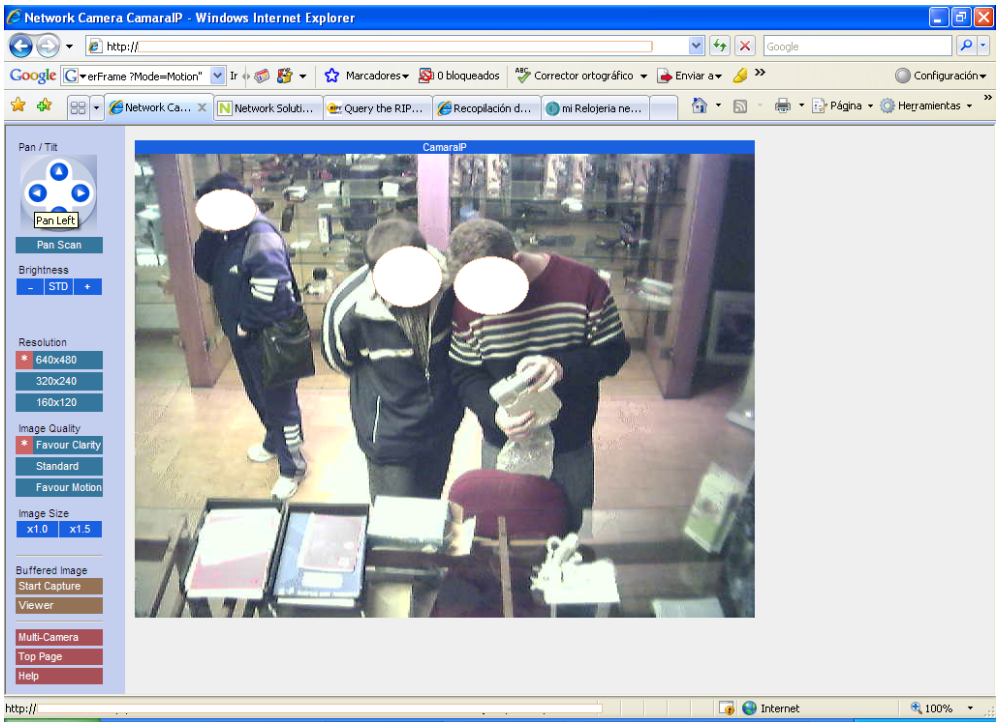
En este caso, la grabación de los trabajadores para difundir sus imágenes a través de Internet con la finalidad citada no constituye una potestad del empresario, puesto que no figura entre las facultades que le reconoce la legislación vigente, por lo que debe de recabar el consentimiento inequívoco y previo de los trabajadores así como de todas aquellas personas cuya imagen pudiera aparecer recabada por las cámaras que para esta finalidad hubiesen sido instaladas.

Deberá tener en cuenta el empresario que el consentimiento anterior podrá ser revocado en cualquier momento por los afectados[19] debiendo el empresario adaptar su sistema de cámaras al consentimiento de éstos.

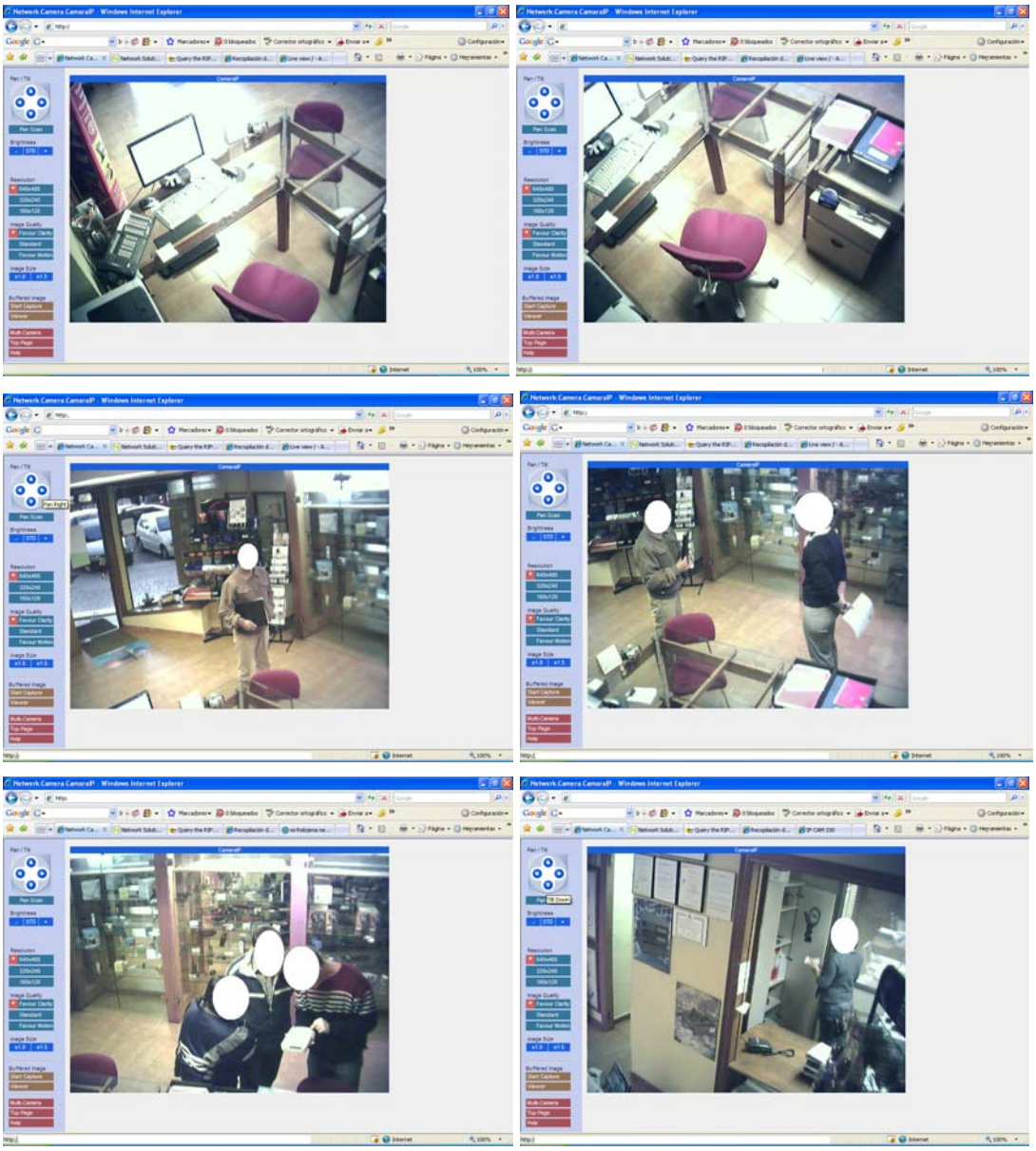
En definitiva, y para finalidades distintas de las de videovigilancia por razones de seguridad o las habilitadas por el Estatuto de los Trabajadores, en cuanto a legitimación se estaría a lo dispuesto en el artículo 6 de la LOPD que requiere que el empresario disponga del consentimiento previo e inequívoco de los empleados quienes podrán revocar dicho consentimiento posteriormente.

5.4. CAPTACIÓN DE IMÁGENES EN EL INTERIOR DE ESTABLECIMIENTOS COMERCIALES.

A modo de ejemplo ilustrativo se han anexado las siguientes imágenes:



[19] El artículo 6.3 de la LOPD establece que "el consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos."



Respecto del principio de legitimación, la captación y difusión de imágenes del interior de locales comerciales que permitan identificar a las personas que se encuentran en su interior requeriría del consentimiento inequívoco y previo de los afectados o de una Ley que lo autorice sin que en este caso sea de aplicación ninguna de las excepciones previstas.

La legitimación que pudiera otorgar el Estatuto de los Trabajadores no sería suficiente, ya que además de empleados, se captarían imágenes de clientes que no se encuentran sujetos a una relación laboral con el titular del establecimiento.

En el caso de que la finalidad fuese por razones de seguridad podría existir legitimación amparada en la Ley 23/1992 de 30 de julio, de Seguridad Privada. Para ello debiera de darse cumplimiento a lo previsto en la citada Ley y adicionalmente a lo establecido en la LOPD en general y a la

Instrucción 1/2006 sobre videovigilancia en particular[20]. En resumen, a los siguientes aspectos:

- En primer lugar y dado el carácter especialmente intrusivo de la videovigilancia dicha medida ha de aplicarse con carácter restrictivo. Es decir, únicamente estaría permitido su uso para el citado fin cuando no hubiere otras medidas alternativas disponibles.
- En segundo lugar, y bajo la hipótesis de que no hubiere otras medidas alternativas disponibles, la instalación de las cámaras debiera de realizarse por una **empresa de seguridad** debidamente acreditada para tal fin por el Ministerio del Interior.
- Adicionalmente, y si las imágenes captadas fueren grabadas habría que proceder por parte del responsable del establecimiento comercial a inscribir dicho fichero en el Registro General de la Agencia.

En el caso de que exista legitimación suficiente, debería de cumplirse también el principio de información ya detallado anteriormente así como los de secreto[21] y seguridad[22] que impediría para dicha finalidad la difusión de las imágenes en abierto a través de Internet.

En el caso de que la finalidad fuese la de dar a conocer el establecimiento, el responsable del mismo habría de recabar el consentimiento inequívoco tanto de todos los clientes como de todos los empleados cuyas imágenes pudieran ser captadas lo que resultaría extremadamente difícil llevar a la práctica. En este sentido hay que tener en cuenta que no se consideraría un consentimiento inequívoco válido la mera entrada de una persona a un local en el que simplemente se informe mediante carteles de la existencia de la

[20] Para más información consultar la guía de videovigilancia disponible en la página web de la Agencia en www.agpd.es. Dicha guía contiene los criterios y pautas a seguir para la utilización de cámaras de vídeo con fines de videovigilancia en consonancia con la normativa de protección de datos, en la medida que capten imágenes de personas identificables, y con la normativa de seguridad privada.

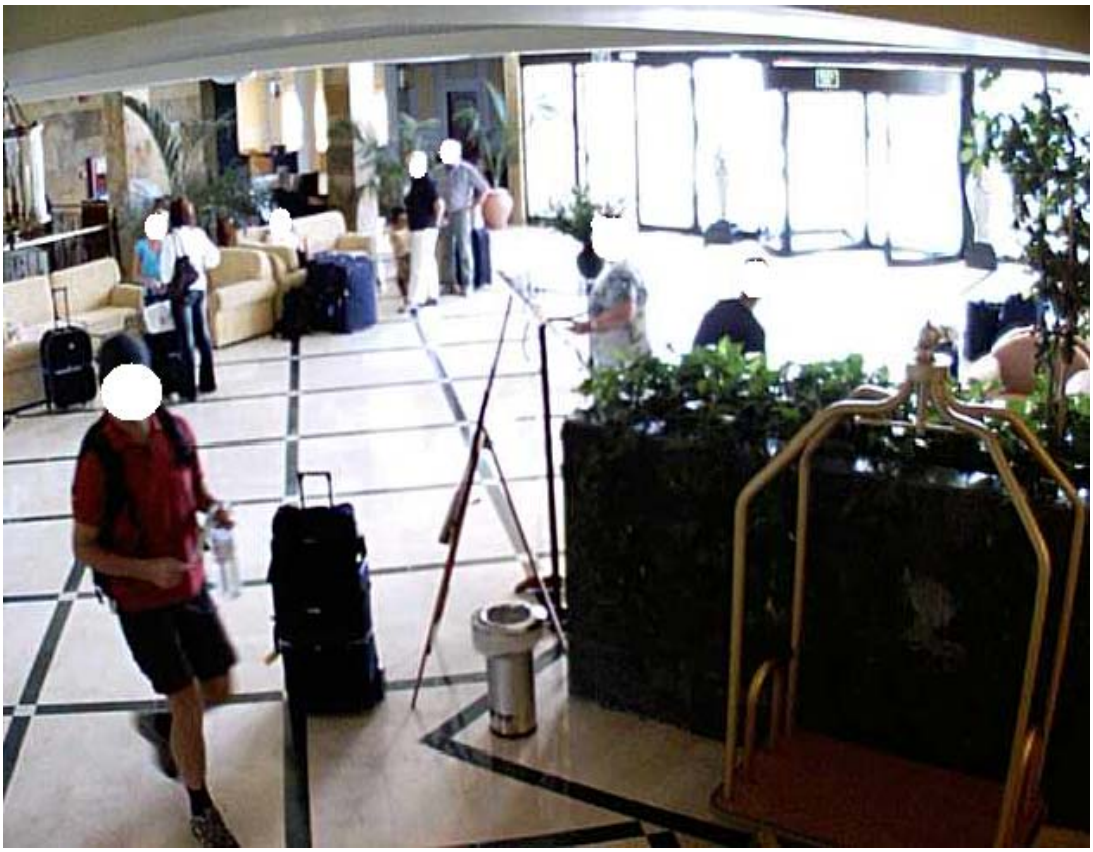
[21] El deber de secreto en la normativa de protección de datos establece que cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas. El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

[22] De acuerdo a la normativa de protección de datos, el responsable del establecimiento comercial deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Por tanto, quien haya contratado los servicios de una empresa de seguridad, -ya sea una empresa, una comunidad de propietarios, etc.-, debe cumplir con el deber de garantizar la seguridad de las imágenes en los términos establecidos por la LOPD y su Reglamento de desarrollo. Es aconsejable consultar la Guía de Seguridad de Datos disponible en el Canal de Documentación del website de la Agencia:

https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/index-ides-idphp.php

grabación y difusión de las imágenes.

Un ejemplo de este supuesto es el que se refleja a continuación y que corresponde al vestíbulo de un hotel cuya imagen se ofrece en abierto a través de Internet.



6. ACTUACIONES DE LA AEPD

La videovigilancia por razones de seguridad ha tenido en los últimos años un crecimiento exponencial como se describe en las Memorias de la Agencia.

Para facilitar que esta actividad se realice cumpliendo las garantías de la normativa de protección de datos se dictó la Instrucción 1/2006, de 8 de noviembre en la que se establecen las reglas para la aplicación de dicha normativa a las especialidades de la videovigilancia. Asimismo, ha impulsado su conocimiento con la publicación de la "Guía sobre videovigilancia" y la celebración de la II Sesión Anual abierta de la Agencia.

Sin embargo, estas iniciativas no han impedido la apertura de procedimientos sancionadores cuando se han constatado vulneraciones de la LOPD.

En 2008 se han resuelto 44 procedimientos sancionadores, lo que supone un incremento del 633% sobre el año anterior.

La tipología de infracciones declaradas comprende la omisión de la información preceptiva sobre la actividad de videovigilancia, el tratamiento de la

imagen de los afectados sin su consentimiento u otra causa que lo legitime y la no inscripción de ficheros de videovigilancia.

Del mismo modo, la Agencia ha reaccionado ante la proliferación del uso de videocámaras en Internet, objeto de la presente inspección sectorial.

En 2009 se han iniciado siete procedimientos sancionadores en este ámbito.

Todos ellos tienen en común la visualización de imágenes de personas identificables, accesibles a cualquier usuario en Internet.

En dos de ellos, los imputados son personas físicas particulares que permitían visualizar las imágenes en la vía pública sin consentimiento de los afectados.

En los restantes procedimientos las imputadas son empresas que han permitido visualizar en sus propios locales imágenes de los empleados o de terceras personas ajenas a la empresa, sin su consentimiento.

En uno de ellos se tratan imágenes de los clientes y de terceras personas en el hall de un hotel.

La LOPD tipifica estas conductas como infracción grave.

7. CONCLUSIONES GENERALES

a. El empleo de las denominadas cámaras IP se ha generalizado de forma considerable en Internet como lo demuestra que muchas de estas cámaras detectadas 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.

b. Parte de las cámaras IP detectadas recogen paisajes o panorámicas que al no recabar imágenes de personas que pudieran ser identificadas o reconocidas no presentan riesgo alguno para la privacidad, pudiendo difundir dichas imágenes en abierto, es decir, sin necesidad de ningún tipo de control de acceso.

c. Otra parte importante de las cámaras IP detectadas recogen imágenes de personas que pudieran ser identificadas detectándose tres situaciones típicas:

    i. Captación de imágenes de la vía pública.

    ii. Captación de imágenes en el lugar de trabajo.

    iii. Captación de imágenes del interior de establecimientos comerciales.

Las tres situaciones detectadas y citadas tienen en común el difundir las imágenes en abierto, es decir, sin ningún tipo de control de acceso, lo que deriva en la práctica en una situación de elevado impacto para la privacidad y por lo tanto de alto riesgo de incumplimiento de la normativa de protección de datos.

Respecto de las captaciones detectadas de imágenes de la vía pública se produce un incumplimiento del principio de legitimación, ya que dicha

captación queda reservada a las Fuerzas y Cuerpos de Seguridad del Estado con fines de videovigilancia. Las imágenes captadas por una persona a título individual son legítimas en la medida que se utilicen únicamente en el marco de una actividad doméstica exclusivamente privada por lo que no podrán ser difundidas a través de Internet.

Respecto de las captaciones detectadas en centros de trabajo y locales comerciales existiría, adicionalmente, riesgo de incumplimiento del principio de legitimación si la captación, fuera de los casos de control de la actividad laboral o de la vigilancia de bienes y personas o videovigilancia, no contará con el consentimiento inequívoco y previo de los afectados: empleados y/o terceros cuya imagen resulte captada.

d. Aun en el caso de contar con la debida legitimación, deberá de tenerse en cuenta las obligaciones derivadas de los principios de información, seguridad y deber de secreto que resulten de aplicación en cada caso.

8. DECÁLOGO PARA USUARIOS DE VIDEOCÁMARAS CONECTADAS A INTERNET

1. Para evitar accesos de terceros no autorizados es esencial que active el control de acceso a las cámaras y a las imágenes con usuario/contraseña, ya que, sin esta precaución, las videocámaras pueden permitir a cualquiera acceder desde Internet.

2. Únicamente las Fuerzas y Cuerpos de Seguridad pueden utilizar videocámaras para vigilar la vía pública.

3. Si va a usar videocámaras por motivos de seguridad privada, - como evitar hurtos, o robos, detectar intrusos, controlar accesos garajes o urbanizaciones etc.- únicamente podrá instalarlas una empresa de seguridad autorizada por el Ministerio del Interior.

4. Si usa videocámaras para controlar la actividad de los trabajadores debe informarles y respetar sus derechos. Si va a difundir imágenes de su empresa con fines promocionales debe obtener el consentimiento de los empleados.

5. El uso de videocámaras para seguridad privada, control laboral y cuando pueda reconocerse la identidad de las personas, deberá cumplir la Ley Orgánica de Protección de Datos y en su caso la Instrucción 1/2006, sobre el tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras. Consulte la Guía de Videovigilancia disponible en el web del la Agencia Española de Protección de Datos (https://www.agpd.es/).

6. Si usa videocámaras emitiendo imágenes de establecimientos como centros comerciales, tiendas, edificios en construcción, hoteles, polideportivos etc. y las personas que aparecen en ellas son reconocibles deberá obtener su consentimiento.

7. Si capta de imágenes panorámicas, -paisajes, edificios, tráfico urbano etc.-, en las que no se

reconozcan personas no está obligado a aplicar las normas de protección de datos. 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.

8. Si usa webcam por razones privadas como realizar videollamadas, chat con vídeo o mostrar imágenes en tiempo real a amistades, tampoco está obligado a aplicar las normas sobre protección de datos.

9. En el caso anterior no olvide proteger su intimidad y active el usuario y contraseña del servicio. No acepte conversaciones con desconocidos ni les facilite acceso a su webcam

10. Asegúrese de que los niños usen estos servicios de modo seguro y controlado. En particular compruebe que los menores realizan un uso apropiado, seguro y bajo su supervisión de las webcam. Consulte la Guía de la AEPD sobre Derechos de niños y niñas y deberes de padres y madres en Internet. (https://www.agpd.es/).

9. RECOMENDACIONES A LOS FABRICANTES Y DISTRIBUIDORES DE VIDEOCÁMARAS CONECTADAS A INTERNET

Incluir junto con la documentación o instrucciones de las cámaras el DECÁLOGO PARA USUARIOS DE VIDEOCÁMARAS CONECTADAS A INTERNET.

Para más información consulte la ***guía de videovigilancia*** disponible en la página web de la Agencia Española de Protección de Datos en www.agpd.es.