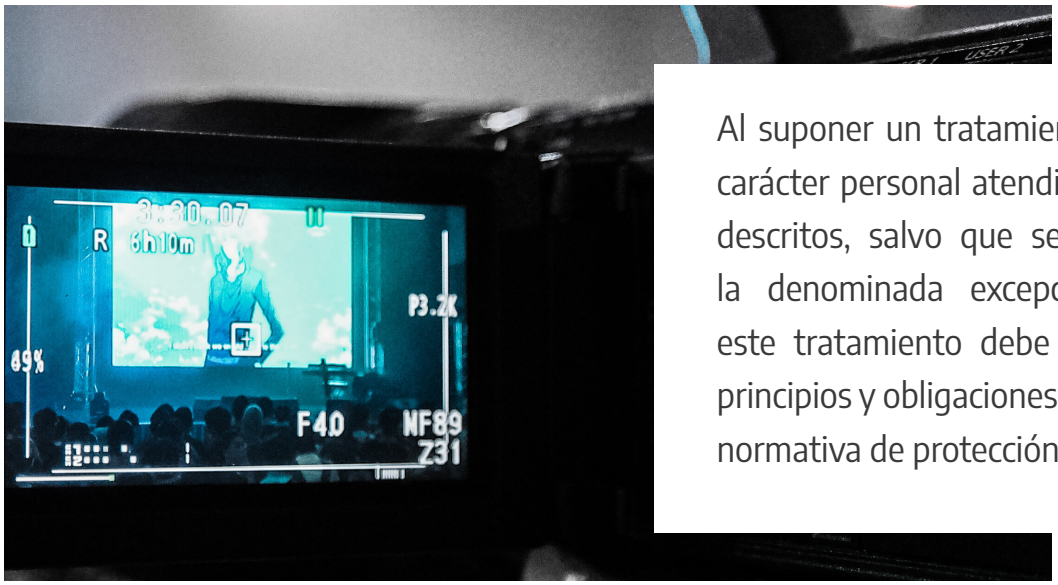
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Guía sobre el uso de videocámaras para seguridad y otras finalidades

Índice

1. Introducción

La imagen de una persona en la medida que identifique o pueda identificar a la misma constituye un dato de carácter personal, que puede ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras con la finalidad de garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines, como la investigación, la asistencia sanitaria o el control de la prestación laboral por los trabajadores.



Al suponer un tratamiento de datos de carácter personal atendiendo a los fines descritos, salvo que sea de aplicación la denominada excepción doméstica, este tratamiento debe ajustarse a los principios y obligaciones que establece la normativa de protección de datos.

Así, una de las cuestiones que más se han planteado ante esta Agencia Española de Protección de Datos (AEPD), tanto por responsables, como por encargados, profesionales y ciudadanos, es la utilización de las cámaras, principalmente con la finalidad de seguridad, y su relación con esta normativa, a los efectos de cumplir con ella y garantizar los derechos de los que son captados.

Para facilitar este cumplimiento, la web de la AEPD cuenta con un apartado específico dedicado a la videovigilancia, donde se pueden consultar diversos materiales al respecto, incluyendo fichas prácticas así como informes jurídicos que analizan supuestos específicos del uso de videocámaras tanto con fines de seguridad como para otros propósitos.

Otro de estos materiales que han sido consultados y utilizados con gran frecuencia es la anterior Guía de Videovigilancia, a la que la presente Guía viene a sustituir.

Este nuevo documento, titulado "Protección de datos: Guía sobre el uso de videocámaras para seguridad y otras finalidades", que forma parte de un conjunto de publicaciones sectoriales, iniciada con las publicaciones de la Guía "Protección de datos y administración de fincas", la Guía "Protección de datos y Administración Local" y "Guía para centros educativos", se divide fundamentalmente en dos apartados:

En primer lugar, se analiza el uso de las videocámaras con fines de seguridad, incluyendo también el análisis de supuestos específicos.

En segundo lugar, se recogen numerosos casos en que las videocámaras se utilizan para finalidades diferentes al de la seguridad.

Por otra parte, y puesto que el Reglamento General de Protección de Datos (RGPD), es aplicable desde el 25 de mayo de 2018, el contenido de esta Guía incluye aquellas cuestiones que afectan al tratamiento realizado mediante cámaras según lo dispuesto en esta norma.

Asimismo, y para una mayor difusión y conocimiento del RGPD, la AEPD ha publicado diversos documentos, entre los que destacan:

- Guía del Reglamento General de Protección de Datos para responsables del tratamiento
- Guía para el cumplimiento del deber de informar
- Directrices para la elaboración de contratos entre responsables y encargados del tratamiento
- Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD
- Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD
- Listado de cumplimiento normativo

Esta Guía se completa con una descripción sobre el tratamiento de imágenes mediante las tecnologías emergentes (como son las denominadas "cámaras on board" así como los drones).

Por último, esta nueva Guía supone una actuación más de las previstas en el Plan Estratégico 2015-2019 de la AEPD, y más concretamente, del Eje 3 "Una Agencia colaboradora, transparente y participativa".

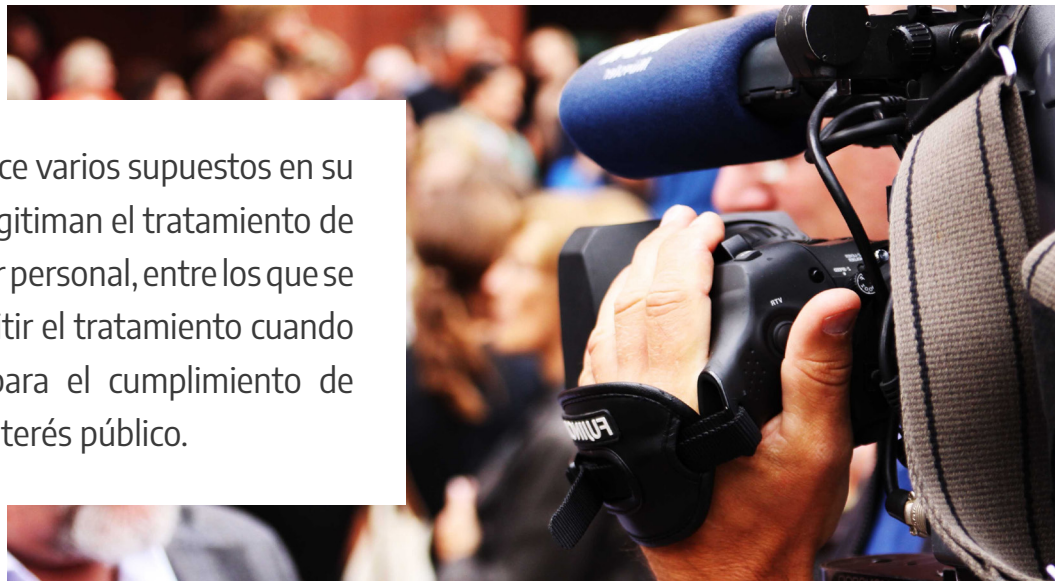
2. Tratamiento de imágenes con fines de seguridad

Cuando se realice el tratamiento de imágenes con fines de seguridad a través de los diversos sistemas existentes de captación, debe valorarse en primer lugar la legitimación para utilizar dichos sistemas de captación, así como los principios de limitación de la finalidad y minimización de datos que recoge la norma en su artículo 5.

Además, y en referencia al principio de responsabilidad proactiva, deben realizarse también una serie de actuaciones para que estos tratamientos se ajusten al contenido del RGPD.

2.1 Legitimación

El RGPD establece varios supuestos en su artículo 6 que legitiman el tratamiento de datos de carácter personal, entre los que se encuentra permitir el tratamiento cuando sea necesario para el cumplimiento de una misión de interés público.



Por lo tanto, y puesto que la finalidad de la videovigilancia consiste en garantizar la seguridad de personas, bienes e instalaciones, el interés público legitima dicho tratamiento. Asimismo, el considerando 45 del RGPD contempla que si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, este tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros.

A este respecto, cabe citar la normativa aplicable a sectores específicos, como es la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos

de Seguridad, y su Reglamento de desarrollo aprobado mediante Real Decreto 596/1999, de 16 de abril, la Ley 5/2014, de 4 de abril, de Seguridad Privada, o la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte así como su reglamento de desarrollo aprobado mediante Real Decreto 203/2010, de 26 de febrero.

2.2 Proporcionalidad

2.2.1 Limitación de la finalidad

El RGPD recoge en su artículo 5 este principio, en virtud del cual, los datos personales será recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines, de manera que los datos que sean objeto de tratamiento a través de la videovigilancia serán tratados para la finalidad que ha motivado la instalación de la misma y que está vinculada a garantizar la seguridad de personas, bienes e instalaciones.

2.2.2. Captación de imágenes de la vía pública

Como regla general, la captación de imágenes con fines de seguridad de la vía pública debe realizarse por las Fuerzas y Cuerpos de Seguridad.

Ya que les corresponde la prevención de hechos delictivos y la garantía de la seguridad en la citada vía pública, de conformidad con lo regulado por Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo.

Sin embargo, sobre esta regla general es posible aplicar alguna excepción:

- En algunas ocasiones para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública, Es decir, las cámaras y videocámaras instaladas con

fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Por lo tanto, las cámaras podrían captar la porción mínimamente necesaria para la finalidad de seguridad que se pretende.

- Será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicas o de infraestructuras vinculadas al transporte.
- Gran parte de la actividad de los ciudadanos se desarrolla en espacios que admiten el acceso al público en general, como centros comerciales, restaurantes, lugares de ocio o aparcamientos. Nos referimos a lugares a los que los ciudadanos pueden tener libre acceso aunque sean de propiedad privada, en los que sus titulares utilizan los sistemas de videovigilancia para garantizar la seguridad de las personas e instalaciones.

2.2.3. Minimización de datos

Otro de los principios que recoge el RGPD en su artículo 5 es el principio de minimización de datos, de forma que los datos objeto de tratamiento sean adecuados, pertinentes y limitados en relación con los fines para los que son tratados.

Además, existen espacios que por sus condiciones podría ser desproporcionado la utilización de la videovigilancia, en vestuarios, taquillas y zonas de descanso de trabajadores.

Por otra parte, el mencionado principio también se proyecta a través del número de cámaras que se pretenda utilizar así como el tipo de las mismas, ya que no es lo mismo la captación de imágenes a través de una cámara fija que la que se realiza mediante las denominadas `domo´, que permite grabaciones de 360 grados, o aquellas que son móviles.

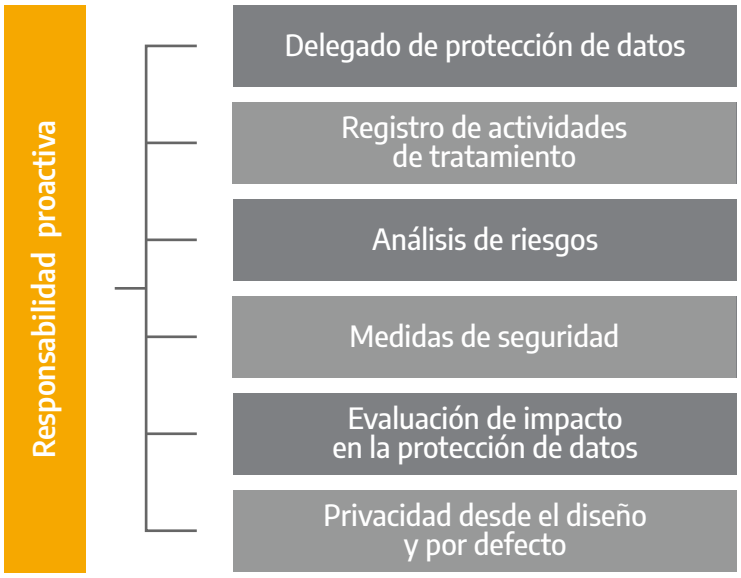
Otra opción para aplicar este principio de minimización de datos es la posibilidad de utilizar las denominadas `máscaras de privacidad´, de tal forma que se evite captar y grabar imágenes excesivas.

- Valore si realmente es necesaria la instalación de la videovigilancia o si el fin perseguido se puede alcanzar de otra forma.
- Cuando realice la instalación, tenga en cuenta la proporcionalidad en función del número de cámaras, tipo de las mismas y la opción de utilizar "máscaras de privacidad".

2.3. Medidas de responsabilidad proactiva

Este concepto, como principio esencial en el tratamiento de datos personales, se establece en el artículo 5 del RGPD al que hemos hecho referencia anteriormente. En concreto, según su apartado 2, la responsabilidad proactiva es una de las obligaciones del responsable del tratamiento en relación a los principios referidos en el apartado 1 del mismo artículo. Por lo tanto, es una de las nuevas obligaciones que se establecen en el RGPD para asegurar el cumplimiento de dichos principios, y que consiste en la capacidad del responsable, es decir, de la organización, de demostrar y proporcionar evidencias de dicho cumplimiento.

El RGPD establece un catálogo de medidas que el responsable y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos son conformes a la norma europea. No obstante, es preciso matizar que no en todos los casos, estas medidas deben aplicarse obligatoriamente.



Además de estas medidas, también debe tenerse en consideración lo siguiente:

- Las relaciones entre responsable y encargado de tratamiento de las imágenes.
- Conservación de las imágenes.
- Derechos de las personas, incluyendo el derecho de información.
- Comunicación de imágenes a terceros.

2.3.1 Delegado de protección de datos

El RGPD introduce como obligatorio la designación de un Delegado de Protección de Datos (DPD) por parte de responsables y encargados en los supuestos regulados en su artículo 37.1.

La norma europea señala que el DPD será una persona con conocimiento especializado en Derecho y la práctica en materia de protección de datos.

Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

En este sentido, y por lo que se refiere al nombramiento del delegado acorde a lo dispuesto en el artículo 37.1 anteriormente citado, y que pueda afectar a la videovigilancia, debemos distinguir:

- Su carácter obligatorio para las Administraciones Públicas. Esta cuestión supone que con independencia de que las Administraciones utilicen la videovigilancia, ya están obligadas a nombrar un DPD.
- Cuando las actividades principales del responsable o encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran de una observación

habitual y sistemática de interesados a gran escala.

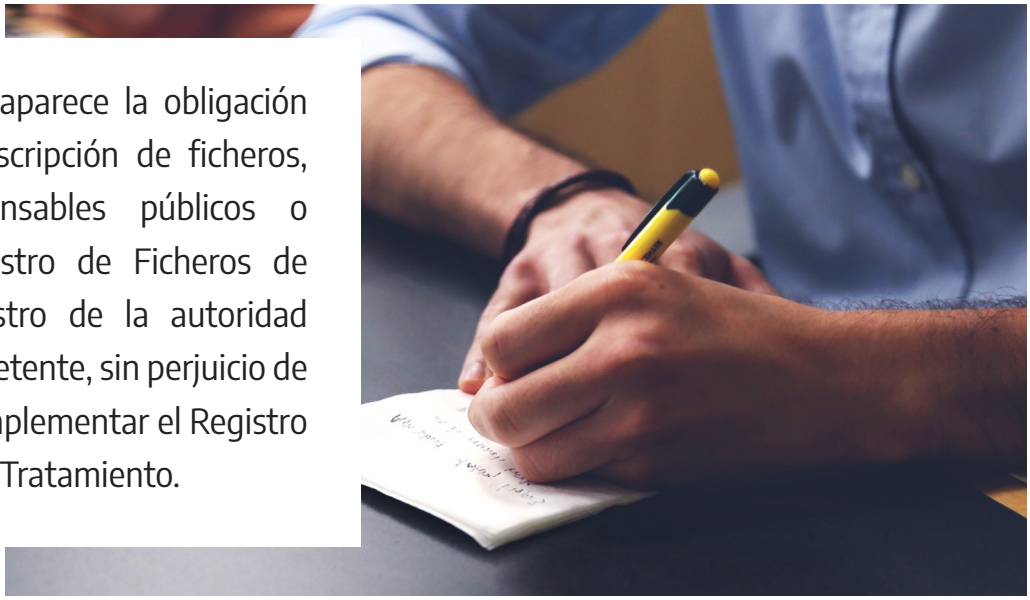
Respecto qué se considera actividad principal, el Grupo de Trabajo del Artículo 29, en su documento `Directrices sobre los delegados de protección de datos´, estima que de conformidad con el considerando 97 del RGPD, se pueden considerar aquellas operaciones clave necesarias para lograr los objetivos del responsable o del encargado.

En el citado documento se incluye como ejemplo al respecto, las empresas de seguridad privada, ya que la vigilancia es la actividad principal de la empresa.

Además, y siendo el tratamiento de datos de la videovigilancia una observación sistemática, debe tenerse en cuenta que estas empresas de seguridad realizan un tratamiento de datos a gran escala tanto cuando actúan como responsables del tratamiento como cuando son encargados.

2.3.2 Registro de actividades de tratamiento

Con el RGPD desaparece la obligación de notificar la inscripción de ficheros, tanto de responsables públicos o privados, al Registro de Ficheros de la AEPD, o registro de la autoridad autonómica competente, sin perjuicio de la obligación de implementar el Registro de Actividades de Tratamiento.



Este Registro podrá organizarse sobre la base de las informaciones de los ficheros notificados al Registro General de Protección de Datos de la AEPD, si bien no es un registro de ficheros sino de tratamientos.

Para configurar este registro de tratamientos, se puede partir de operaciones de tratamiento concretas a una finalidad básica común de todas ellas, así como de los ficheros que ya se encuentre inscritos. Aplicado este registro al tratamiento que se realiza con las cámaras, supondrá que la operación de tratamiento es la videovigilancia ligada a la finalidad de garantizar la seguridad.

Por tanto, los responsables y encargados de tratamientos deben mantener este Registro de Actividades de Tratamiento por escrito, incluso en formato electrónico, en el que se incluya una descripción de los tratamientos de datos de videovigilancia que realicen con la siguiente información.

Registro de actividades: Videovigilancia

Responsable	Nombre y datos de contacto del responsable (o respresentante)
Actividad de tratamiento	Videovigilancia
Legitimación del tratamiento	Artículo 6.1.e del RGPD: Cumplimiento de una misión de interés público
Fines del tratamiento	Garantizar la seguridad de personas, bienes e instalaciones
Nombre y datos del contacto del Delegado de Protección de Datos *(en el caso de que existiese)*	Correo electrónico del contacto Dpd@xxxxxxxxx.es/Dirección física
Categorías de datos personales	Imagen
Categorías de afectados	Por ejemplo ciudadanos, clientes, trabajadores...
Descripción de las medidas técnicas y organizativas de seguridad	Descripción de las mismas
Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales	Fuerzas y Cuerpos de Seguridad. Juzgados y Tribunales
Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.	No existen (como regla general)
Cuando sea posible, plazos previstos para las supresión de las diferentes categorías de datos	Transcurrido un mes, salvo comunicación a Fuerzas y Cuerpos de Seguridad, o/y Juzgados y Tribunales

Aunque se trate de un documento interno que deben elaborar responsables y encargados, el mismo tiene que estar en todo momento a disposición de la Autoridad de Control de protección de datos por si lo requiriese.

No obstante, en el caso de las Administraciones públicas, y vinculado al principio de transparencia administrativa, su registro de actividades de tratamiento sí debe ser objeto de publicación, ya sea en la sede electrónica o en el correspondiente Portal de Transparencia.

Por otra parte, en aquellos supuestos en que el sistema utilizado no grabe o almacene las imágenes (**cámaras que permiten el visionado el tiempo real** pero no realizan grabación alguna), que con la Ley Orgánica 15/1999, de 13 de diciembre, al no existir fichero no tenían la obligación de realizar la inscripción, con el RGPD sí deben configurar este registro, ya que existe un tratamiento.

- Con la aplicación del RGPD desde el 25 de mayo de 2018, la obligación de inscripción de ficheros desaparece.
- El RGPD introduce que los responsables lleven un registro de las actividades de los tratamientos que realicen, en el que se deberá incluir determinada información, como por ejemplo, los fines del tratamiento, las categorías de datos personales o las medidas de seguridad.
- Los encargados de tratamientos también deberán implementar su respectivo registro. Es decir, las empresas de seguridad tienen que elaborar su registro de actividades en relación con su actividad como encargado respecto a cada responsable.

Por último, indicar que si se tratase de cámaras simuladas o ficticias no sería necesario elaborar este registro ni cumplir con el resto de obligaciones del RGPD, ya que no existiría un tratamiento de datos de carácter personal.

2.3.3 Análisis de riesgos y medidas de seguridad

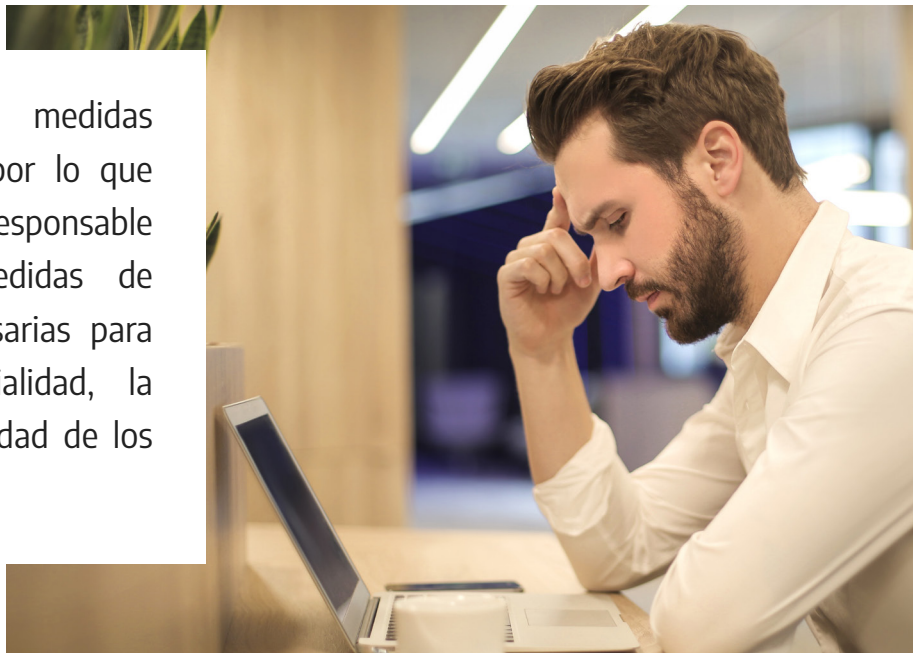
El RGPD obliga a que los responsables lleven a cabo una valoración del riesgo de los tratamientos que realicen, con el fin de establecer las medidas a aplicar.

Este análisis del riesgo variará en función de:

- Los tipos de tratamiento
- La naturaleza de los datos
- El número de afectados
- La cantidad y variedad de tratamientos que realice una misma organización

A través de este análisis de riesgos se determinarán las medidas de seguridad a aplicar en los tratamientos de datos que se lleven a cabo.

El RGPD no establece medidas de seguridad estáticas, por lo que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.



El anterior Título VIII del Real Decreto 1720/2007 establecía unos controles mínimos de obligado cumplimiento para garantizar la seguridad de los datos que se incorporan a los controles o medidas de seguridad que habrá que tener en cuenta en el RGPD dentro de los procesos de análisis de riesgos, por lo que las medidas de seguridad ya existentes se deben mantener y revisar en el marco de dichos procesos. En ningún caso el RGPD se debe entender como la eliminación automática de todas las medidas de seguridad ya existentes.

Así, según el artículo 32 del RGPD, las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

En definitiva el primer paso para determinar las medidas de seguridad será la evaluación del riesgo a la que anteriormente nos hemos referido, y una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

Por otra parte, lo previsto en el Esquema Nacional de Seguridad es aplicable a cualquier información de las Administraciones Públicas sin distinción del soporte en el que se encuentre, por lo que en cuanto a las medidas de seguridad se refiere, este esquema es acorde al enfoque de riesgo del RGPD y se constituye en una herramienta válida para la gestión del riesgo y la adopción de las medidas de seguridad en las citadas Administraciones.

Por tanto, la implementación de las medidas de seguridad cuando se lleve a cabo un tratamiento de datos mediante el uso de la videovigilancia dependerá del análisis de riesgo llevado a cabo previamente.

No obstante, cuándo se trate de tratamientos de videovigilancia que entrañen un escaso riesgo, como podría ser el caso de uso en comunidades de propietarios o pequeños establecimientos, puede utilizarse la herramienta de esta AEPD denominada **FACILITA_RGPD**.

RECUERDE

Para facilitar esta labor puede consultar la **Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD**.

2.3.4 Notificación de brechas de seguridad

Cuando se produzca una brecha de seguridad que afecte a los tratamientos de cámaras con fines de seguridad, es decir, la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos, el responsable del tratamiento que sufra dicha brecha, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo:

- A la AEPD, en un plazo máximo de 72 horas.

  Contenido mínimo de la comunicación de la brecha de seguridad a la AEPD
  - naturaleza de la brecha de seguridad:
    - categorías de afectados (pj. menores, discapacitados, empleados, ciudadanos)
    - número aproximado de afectados
    - categorías de datos comprometidos (pj. identificativos, salud, laborales)
    - número de registros de datos personales afectados
  - nombre y datos de contacto del Delegado de Protección de Datos
  - posibles consecuencias de la brecha de seguridad sufrida
  - medidas adoptadas o propuestas para remediar esta brecha

- Sin perjuicio de lo anterior, a efectos de notificación y en el ámbito de las Administraciones Públicas se tendrán en cuenta las obligaciones derivadas del **Esquema Nacional de Seguridad** y las **Instrucciones Técnicas aplicables**.

Por otra parte, si el encargado del tratamiento de las imágenes sufre una brecha de seguridad, éste debe notificar sin dilación al responsable la existencia de la misma. El RGPD no indica ni el formato de dicha notificación ni el plazo máximo para que se realice dicha notificación, ya que el plazo establecido para el responsable se fija a partir del conocimiento de la brecha de seguridad. Por lo tanto, el responsable deberá fijar las obligaciones de notificación del encargado, de tal forma que le permitan cumplir con los requisitos que a dicho responsable sí obliga el RGPD, en particular, en relación a los datos que es necesario notificar a terceros.

- Los responsables que realicen este tipo de tratamientos pueden elaborar una Plan de Contingencias con la finalidad de mitigar los daños cuando se produzca una brecha de seguridad.
- También deben mantener un registro de los incidentes de seguridad.

Especial consideración merecen las denominadas 'cámaras IP´, que 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.

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, 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.

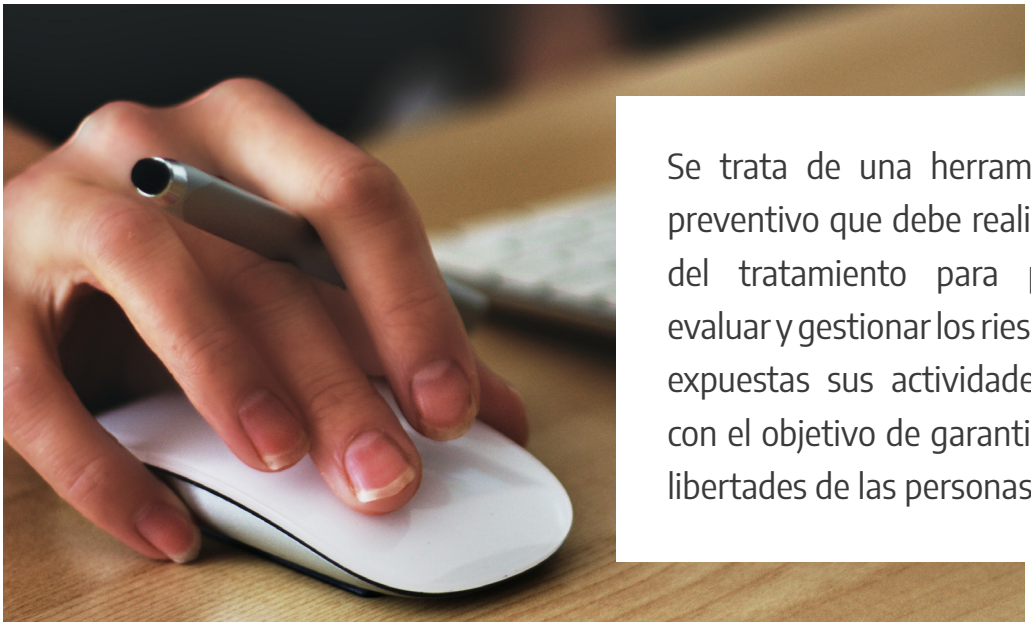
Esta situación, que en si misma pudiera considerarse de riesgo limitado dado el tamaño de la Red, resulta en la práctica de un riesgo elevado como consecuencia de los buscadores, y además, supondría una brecha de seguridad.

RECUERDE

Antes de poner en funcionamiento una 'cámara IP´:

- verifique el control de accesos para proceder a su activación
- cambie el usuario y contraseña que venga asignado por defecto

2.3.5. Evaluación de impacto en la protección de datos



Se trata de una herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

El RGPD señala también que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entraña un alto riesgo para los derechos y libertades, el responsable realizará, antes del tratamiento, una evaluación de impacto. Si se trata de operaciones similares que supongan riesgos similares, se podrá realizar una única evaluación.

Sobre las operaciones que requieran una evaluación de impacto de acuerdo a lo dispuesto en el párrafo anterior, la Autoridad de Control establecerá y publicará una lista al respecto.

Igualmente, podrá publicar otra lista respecto a aquellos tratamientos que no requieran dicha evaluación de impacto.

Además, el RGPD determina los supuestos en que debe realizarse una evaluación de impacto:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
- Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9.1 o de los datos personales relativos a condenas e infracciones penales del artículo 10.
- Observación sistemática a gran escala de una zona de acceso público.

En este sentido, y aplicando los supuestos anteriormente descritos al uso de la videovigilancia, podrían existir tratamientos que requieran con carácter previo a su puesta en funcionamiento la realización de una evaluación de impacto de la protección de datos.

Para determinar estos dos elementos, podemos acudir a las Directrices sobre la evaluación de impacto relativa a la protección de datos del Grupo del Artículo 29, que consideran lo siguiente:

- **Observación sistemática:** tratamiento usado para observar, supervisar y controlar a los interesados. Este tipo de observación representa un criterio porque los datos personales pueden ser recogidos en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando sus datos y cómo se usarán. Además, puede resultar imposible para las personas evitar ser objeto de este tipo de tratamientos en espacios públicos (o espacios de acceso público).

- **Tratamiento de datos a gran escala:** el RGPD no define qué se entiende por gran escala aunque el considerando 91 ofrece alguna orientación. De esta forma, para valorar si el tratamiento se realiza a gran escala se recomienda tener en cuenta los siguientes factores:
  - Número de interesados afectados, bien como cifra o como proporción de la población correspondiente.
  - El volumen de datos o la variedad de elementos de datos distintos que se procesan.
  - La duración, o permanencia, de la actividad de tratamiento de datos.
  - Alcance geográfico de la actividad de tratamiento.

Por lo tanto, y a los efectos de realizar las EIPD en videovigilancia, cuyo tratamiento supone una observación sistemática, el elemento que determinará la necesidad o no de su realización es que dicho tratamiento sea a gran escala.

Por ejemplo, y atendiendo a los criterios para determinar que existe gran escala, podría darse en la utilización de la videovigilancia en espacios de acceso público como pueden ser plazas, calles o grandes centros comerciales.

Asimismo, el mencionado documento del Grupo del Artículo 29 también se refiere a la necesidad de realizar una evaluación de impacto de la protección de datos, en base al artículo 35.1 del RGPD, cuando se utilicen nuevas tecnologías, que pueda implicar un alto riesgo para derechos y libertades de las personas.

De esta forma, podría ser necesaria la evaluación cuando se utilicen drones con fines de seguridad, o bien el tratamiento con fines de videovigilancia sea complementario con otros sistemas como pueden ser el reconocimiento facial o la huella dactilar para el control de acceso a instalaciones.

- Una de las cuestiones básicas a tener en cuenta en la realización de una evaluación de impacto es la participación del delegado de protección de datos.
- Puede consultar la Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD, que puede utilizarse como referencia para realizar una EIPD.

2.3.6 Privacidad desde el diseño y por defecto

El RGPD contiene dos principios para la implementación efectiva de la responsabilidad proactiva, como son los de protección de datos desde el diseño y protección de datos por defecto.

El principio de **protección de datos desde el diseño** supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo.

Por supuesto, estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

Un ejemplo de dichas medidas, que se establece de forma expresa en el RGPD, es que el propio tratamiento incorpore medidas para la seudonimización de los datos personales o la minimización de datos.

Por su parte, la **protección de datos por defecto** supone que se adopten las medidas técnicas y organizativas apropiadas para garantizar que, como su nombre indica, por defecto, sólo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento.

En particular, se destaca como uno de los principios de protección de datos por defecto que los datos no sean accesibles a un número indeterminado de personas físicas, sin la intervención del sujeto de los datos.

Además, debe tenerse en cuenta lo siguiente respecto a la protección de datos por defecto:

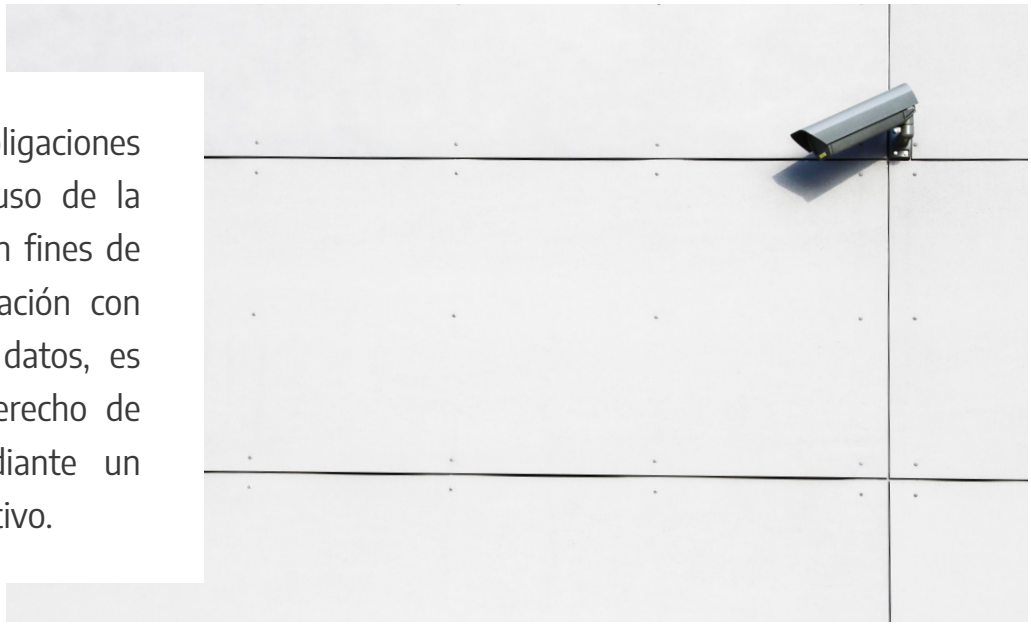
- **Recogida de datos:** analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario.
- **Tratamiento de los datos:** analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos.
- **Conservación:** implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios.
- **Accesibilidad:** limitar el acceso por parte de terceros a dichos datos personales.

Sobre estos elementos aplicados al tratamiento de datos en videovigilancia, al principio de esta Guía nos hemos referido al principio de minimización. La conservación de las imágenes se analiza más adelante en otro apartado.

Asimismo, y sobre la accesibilidad, se debe determinar quién puede acceder a las imágenes así como para qué fines. Todo ello debe estar debidamente documentado.

2.3.7 Derecho de información

Otra de las obligaciones que conlleva el uso de la videovigilancia con fines de seguridad, en relación con la protección de datos, es cumplir con el derecho de información, mediante un distintivo informativo.



Este distintivo se exhibirá en lugar visible, y como mínimo, en los accesos a las zonas vigiladas ya sean interiores o exteriores. En caso que el espacio videovigilado disponga de varios accesos deberá disponerse de dicho distintivo de zona videovigilada en cada uno de ellos.

El distintivo de zona videovigilada deberá informar acerca de:

- La existencia del tratamiento (videovigilancia).
- La identidad del responsable del tratamiento o del sistema de videovigilancia, y la dirección del mismo.
- La posibilidad de ejercitar los derechos reconocidos en los artículos 15 a 22 del RGPD.
- Dónde obtener más información sobre el tratamiento de los datos personales.
- Asimismo, también se pondrá a disposición de los interesados el resto de la información que debe facilitarse a los afectados en cumplimiento del derecho de información regulado en el RGPD.

Para facilitar la adecuación de los tratamientos a lo dispuesto en el RGPD, la AEPD ha editado la Guía para el cumplimiento del deber de informar, en la que se explica cómo cumplir con este derecho, a través del denominado sistema de "dos capas", debido al tipo de información que deben facilitar los responsables en relación con los diferentes tratamientos de datos personales de los interesados que realicen.

- Puede utilizar el siguiente "**Cartel informativo**".
- Para más información, consulte el siguiente **informe jurídico**.

2.3.8 Encargado de tratamiento: contratación de un tercero para el tratamiento de imágenes

El acceso a las imágenes de las cámaras por cuenta de terceros distintos del responsable del tratamiento deberá estar regulado por la existencia de un contrato.

El acceso a las imágenes de las cámaras por cuenta de terceros distintos del responsable del tratamiento deberá estar regulado por la existencia de un contrato.

Por ejemplo, cuando una entidad que ha instalado cámaras de videovigilancia, encarga a un tercero la gestión de las mismas, facilitando el acceso a las imágenes, deberá existir un contrato u otro acto jurídico con arreglo al Derecho de la Unión Europea, en el que se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Asimismo, el RGPD determina el contenido mínimo de este contrato o acto jurídico, y que deberá de adaptarse a las circunstancias concretas de la prestación de los servicios y no ser una simple copia del contenido de las cláusulas del artículo 28.3 del RGPD y cuyo objetivo será garantizar el cumplimiento de la norma de acuerdo con las instrucciones del responsable.

Este contenido del contrato u acto jurídico de encargado de tratamiento, de forma resumida, sería el siguiente:

- Las instrucciones del responsable del tratamiento
- El deber de confidencialidad
- Las medidas de seguridad
- El régimen de la subcontratación
- La forma en que el encargado asistirá al responsable en el cumplimiento de responder el ejercicio de los derechos de los afectados
- La colaboración en el cumplimiento de las obligaciones del responsable
- El destino de los datos al finalizar la prestación

Por otra parte, el responsable debe elegir un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del responsable. El Considerando 81 del RGPD prevé que el encargado del tratamiento debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento, incluida la seguridad del tratamiento, así como del cumplimiento de la normativa de protección de datos.

- Los contratos con encargados de tratamiento, anteriores a la aplicación del RGPD (25 mayo 2018), en la medida de lo posible, deben ir adecuándose.
- Para facilitar esta adaptación puede consultar:
  - Guía del Reglamento General de Protección de Datos para responsables de Tratamiento (página 15)
  - Directrices para la elaboración de contratos entre responsables y Encargados del tratamiento
- Para demostrar que el encargado ofrece garantías suficientes, el RGPD prevé que la adhesión a códigos de conducta o a un mecanismo de certificación sirva como mecanismos de prueba.

Por otra parte, aquellos sistemas de videovigilancia que vayan a estar conectados con una central receptora de alarmas o un centro de control, deberán cumplir lo previsto en la Ley de Seguridad Privada y demás normativa aplicable. En concreto, requerirán la prestación de servicios que únicamente pueden ser realizados por empresas de seguridad en virtud de sus condiciones y cualificación.

En este sentido, y respecto a la prestación de este tipo de servicios por las empresas de seguridad, éstas tendrán la condición de encargado de tratamiento.

Sin embargo, si la empresa de seguridad gestiona el sistema de videovigilancia en el domicilio de las personas físicas, adquiere la condición de responsable del tratamiento.

- Para más información sobre la determinación de responsable o encargado en relación con las empresas de seguridad, consulte el siguiente **informe jurídico**.

2.3.9 Conservación de imágenes

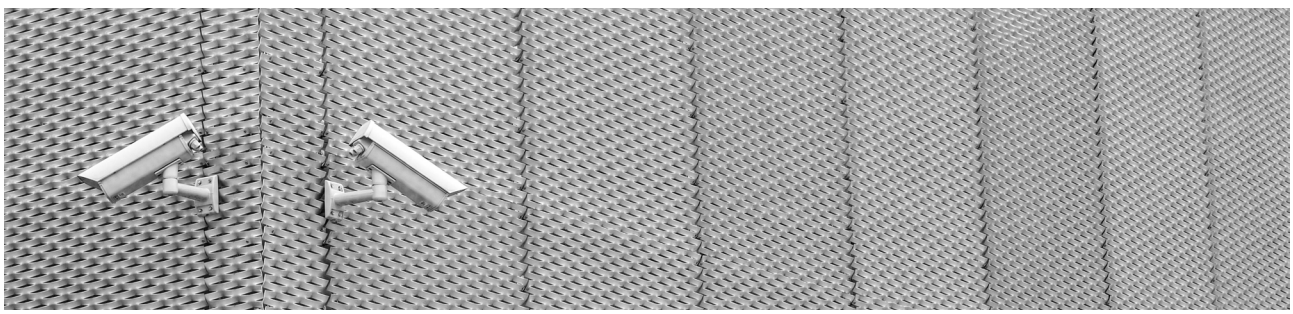
Con la aplicación del RGPD desde el 25 de mayo de 2018, debe considerarse que la mayor parte de la Instrucción 1/2006 ha quedado desplazada, ya que el contenido de la misma, como puede ser la legitimación o los derechos de las personas, queda desplazado por lo establecido al respecto por la norma europea.

Además, con el RGPD desaparece la obligación de inscribir ficheros a los que se refiere la Instrucción 1/2006.

No obstante, puede considerarse que queda en vigor lo dispuesto en el artículo 6 de la citada instrucción que regula el plazo de conservación, y que se refiere a que se produzca la cancelación de imágenes en el plazo máximo de un mes.

Sin embargo, una interpretación acorde con el RGPD, ya que este no contempla la cancelación sino la supresión, supone que ese plazo de conservación de máximo de un mes no será de cancelación sino de supresión, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

A mayor abundamiento con el criterio descrito anteriormente, existen normas específicas que así lo contemplan como la **Ley Orgánica 4/1997** o el **Reglamento que desarrolla la Ley contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte**, en las que transcurrido el plazo máximo de un mes, debe producirse el borrado de las imágenes.



2.3.10 Derechos de las personas

Los artículos 15 a 22 del RGPD regulan los derechos que los afectados que pueden ejercitar ante los responsables y encargados (en este último caso, cuando así se haya previsto entre el responsable y el encargado): acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición, y oposición a decisiones individuales automatizadas.

No obstante, el ejercicio de estos derechos debe ser matizado en el ámbito de la videovigilancia.

En primer lugar, no resulta posible el ejercicio del derecho de rectificación ya que por la naturaleza de los datos -imágenes tomadas de la realidad que reflejan un hecho objetivo-, se trataría del ejercicio de un derecho de contenido imposible.

En segundo lugar, tampoco sería aplicable el derecho de portabilidad ya que, aunque se trata de un tratamiento automatizado, la legitimación no se basa ni en el consentimiento ni en la ejecución de un contrato.

En tercer lugar, no se aplicaría parte del contenido del derecho a la limitación del tratamiento, en su aspecto de "cancelación cautelar" que está vinculada al ejercicio de los derechos de rectificación y oposición.

Por otra parte, sí serían aplicables los siguientes derechos:

- El derecho de acceso, si bien éste reviste características singulares, ya que requiere aportar como documentación complementaria una imagen actualizada que permita al responsable verificar y contrastar la presencia del afectado en sus registros. Resulta prácticamente imposible acceder a imágenes sin que pueda verse comprometida la imagen de un tercero. Por ello puede facilitarse el acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

  Si se ejerciese el derecho de acceso ante el responsable de un sistema que únicamente reproduzca imágenes sin registrarlas (visionado de imágenes en tiempo real) deberá responderse en todo caso indicando la ausencia de imágenes grabadas.
- El derecho de supresión, al que nos hemos referido anteriormente en relación con la supresión de las imágenes en el plazo máximo de un mes, sin perjuicio de la excepción referida
- El derecho a la limitación del tratamiento, que se aplicaría en su otra vertiente, es decir, se solicite al responsable que se conserven las imágenes cuando:
  - El tratamiento de datos sea ilícito y el interesado se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso.

- El responsable ya no necesite los datos para los fines del tratamiento pero el interesado si los necesite para la formulación, ejercicio o defensa de reclamaciones.

2.3.11 Comunicación de imágenes a terceros

En el ámbito que nos ocupa este tipo de comunicaciones sin consentimiento de los interesados ocurren con mayor frecuencia en los siguientes casos:

- Cuando la comunicación de imágenes tengan por destinatarios los Jueces o Tribunales.
- Cuando las Fuerzas y Cuerpos de Seguridad soliciten las grabaciones en aquellos supuestos que son necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

A los efectos de la legitimación para comunicar estos datos, en el primero de los supuestos descritos se aplicaría el cumplimiento de una obligación legal en base a lo recogido en el artículo 236 quáter de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

En el segundo, el RGPD determina en su artículo 2.2.d) su no aplicación al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención, y que según su considerando 19, la protección de las personas físicas relativas a este tipo de tratamientos es objeto de un acto jurídico específico a nivel de la Unión.

Dicho acto lo constituye la **Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016**, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, ya la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI, contempla en su artículo 8, apartado 1, relativo a la licitud del tratamiento, que los Estados miembros dispondrán que el tratamiento solo sea lícito en la medida en que sea necesario para la ejecución de una tarea realizada por la autoridad competente, para los fines establecidos en el artículo 1, apartado 1, y esté basado en el Derecho de la Unión o del Estado miembro.

Según el considerando 12 de esta Directiva, se trata de las actividades realizadas por la Policía u otras fuerzas y cuerpos de seguridad, que también pueden incluir el ejercicio de autoridad mediante medidas coercitivas, como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios, así como el mantenimiento del orden público.

No obstante lo anterior, la citada Directiva no ha sido todavía transpuesta al ordenamiento jurídico español, por lo que si bien el RGPD desplaza la mayor parte del contenido de la LOPD, y con la finalidad de que las comunicaciones de datos realizadas a las Fuerzas y Cuerpos de Seguridad gocen de cobertura normativa, seguirá siendo aplicable lo dispuesto en el artículo 22 de la anteriormente citada LOPD.

En todo caso, la petición de las grabaciones en los supuestos descritos debe realizarse de forma motivada, y la entrega de las mismas debe ser proporcional a la finalidad del requerimiento realizado, sin que se produzca una comunicación indiscriminada.

Por otra parte, en ocasiones, los particulares solicitan acceder a determinadas imágenes grabadas por las cámaras de videovigilancia, para conocer la identidad de un tercero, a los efectos de poder ejercitar determinadas acciones judiciales y/o contractuales.

Este acceso se caracteriza por lo siguiente:

- **Legitimación:** el interés legítimo invocado debe referirse al ejercicio del derecho fundamental a la tutela judicial efectiva, en la medida que las imágenes se utilizarán para la obtención de pruebas para formular una posterior denuncia por delito, o reclamación por responsabilidad contractual, o extracontractual a una compañía de seguros
- **Finalidad compatible:** esta comunicación de datos no persigue una finalidad diferente con la que se recogieron los datos, pues entra dentro del término amplio de "seguridad", a los efectos descritos en el párrafo anterior
- **Minimización de datos:** la cesión o comunicación de las imágenes de terceros debe limitarse al mínimo necesario para la finalidad pretendida, en la medida que el solicitante pueda determinar exclusivamente lo relacionado con el incidente concreto y específico a que se refiera su petición.

En todo caso, se recuerda que, de conformidad con la **Ley de Enjuiciamiento Criminal** (artículos 259, 262 y 264) quien presencie la comisión de un delito debe comunicarlo a la Policía, Fiscalía o Tribunales.

- Para más información puede consultar estos informes jurídicos: **I** y **II**

3. Supuestos específicos de tratamiento de imágenes con fines de seguridad

En el ámbito de la videovigilancia, el fin más comúnmente perseguido, como ya se ha indicado es garantizar la seguridad de personas e instalaciones.

La legislación vigente habilita el uso de videocámaras en el contexto de la seguridad pública y de la seguridad privada.

Respecto a las videocámaras instaladas en espacios públicos, habrá que acudir a la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Por su parte, la Ley 5/2014, de 4 de abril, de Seguridad Privada hace referencia a la utilización de cámaras de videovigilancia en espacios privados.
También existe otra normativa de ámbito más específico que habilita al uso de la videovigilancia, como puede ser la referente al sector de los espectáculos deportivos.

3.1 Fuerzas y Cuerpos de Seguridad

La instalación de videocámaras en lugares públicos, tanto fijas como móviles, es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, rigiéndose el tratamiento de dicha imágenes por su legislación específica, contenida en la Ley Orgánica 4/1997, de 4 de agosto, y su Reglamento de desarrollo, sin perjuicio de que les sea aplicable, en su caso, lo especialmente previsto en el RGPD, en aspectos como la adopción de las medidas de seguridad que resulten de la realización del análisis de riesgos así como el registro de actividades de tratamientos.

Su utilización en lugares públicos tienen una finalidad específica de seguridad en beneficio de la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La instalación de este tipo de dispositivos de las imágenes grabadas están sujetas a requisitos muy estrictos ya que, en primer lugar, la autorización de instalación de videocámaras fija y la utilización de cámaras móviles, se otorga por la Delegación del Gobierno previo informe preceptivo y vinculante de la Comisión de Garantías de la Videovigilancia de la Comunidad Autónoma correspondiente.

Dicha autorización tendrá una vigencia máxima de un año, debiendo renovarse una vez finalizado éste, llevando las Comisiones de Videovigilancia un registro de instalaciones autorizadas.

Para autorizar su instalación se tendrá en cuenta, conforme al principio de proporcionalidad, los criterios de intervención mínima e idoneidad de manera que:

- Sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en la Ley.
- Se deberá ponderar, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.
- Su utilización exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.
- No se podrán utilizar para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni en lugares en lugares públicos, abiertos o cerrados, cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada.

RECUERDE

Estas mismas reglas se aplicarán en el caso de que se quieran utilizar cámaras propias o teléfonos móviles de las Fuerzas y Cuerpos de Seguridad. Para más información consulte este **informe jurídico**.

Asimismo, serán de aplicación también las siguientes reglas:

- Las imágenes captadas deberá ponerse a disposición de la autoridad administrativa o judicial competente.
- Se fija en un mes el periodo de conservación de las imágenes, transcurrido el cual deberán destruirse, salvo que estén relacionadas con infracciones penales o administrativas en materia de seguridad pública o con una investigación policial en curso.
- El acceso a las grabaciones deberá observar la debida reserva, confidencialidad y deber de secreto en relación con las mismas.
- Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos.
- Las zonas vigiladas deberán estar señalizadas.
- Las personas interesadas podrán ejercer el derecho de acceso y cancelación de las imágenes en que hayan sido recogidas.

3.2 Infraestructuras críticas

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, establece una serie de requisitos para las infraestructuras críticas ubicadas en el territorio nacional vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.

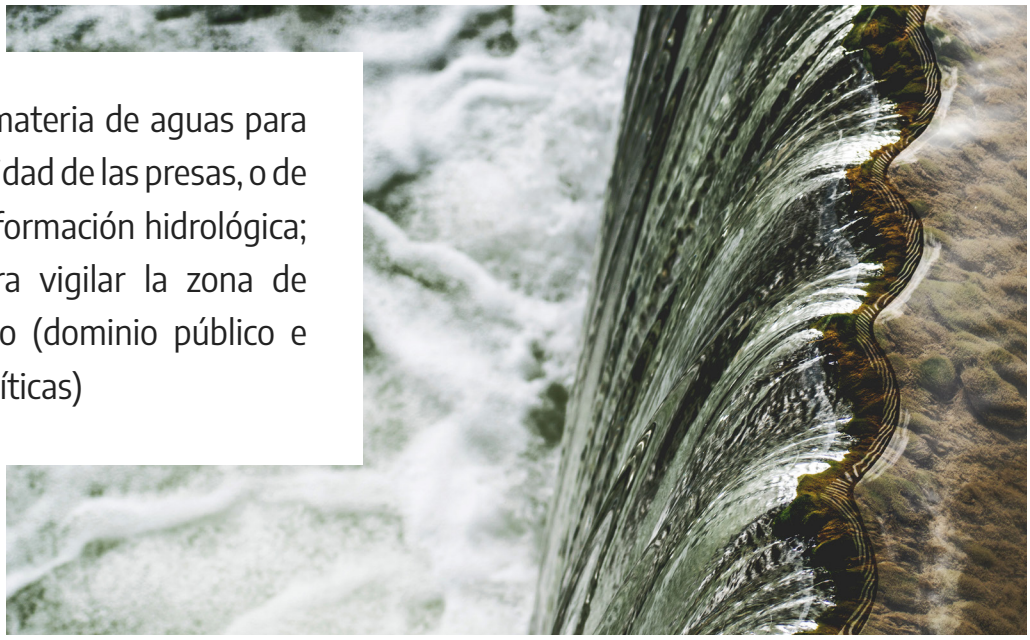
Se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.

El Ministerio del Interior, a través de la Secretaria de Estado de Seguridad, es el responsable del Catálogo Nacional de Infraestructuras Estratégicas, y tiene la competencia para clasificar una infraestructura como estratégica, y en su caso, corno infraestructura crítica o infraestructura crítica europea, así como para incluirla en el Catálogo.

A la instalación de un sistema de videovigilancia utilizado para proteger una infraestructura crítica le es de aplicación el RGPD.

También pueden existir casos especiales previstos por las leyes que permiten la videovigilancia en espacios públicos. Por ejemplo, en materia de dominio público las leyes especiales aplicables pueden prever determinadas obligaciones para las entidades públicas competentes.

Como sucede en materia de aguas para preservar la integridad de las presas, o de los sistemas de información hidrológica; o en puertos para vigilar la zona de servicio del puerto (dominio público e Infraestructuras críticas)



3.3 Espectáculos deportivos

La Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, así como su Reglamento de desarrollo, establece que, por razones de seguridad, las personas organizadoras de las competiciones y espectáculos deportivos que determine la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte, deberán instalar circuitos cerrados de televisión para grabar el acceso y el aforo completo del recinto deportivo, inclusive los aledaños en que puedan producirse aglomeraciones de público. Además, adoptarán las medidas necesarias para garantizar su buen estado de conservación y correcto funcionamiento.

La instalación de los dispositivos de videovigilancia así como el tratamiento de las imágenes resultantes, se encuentran sometidos a lo dispuesto en la Ley Orgánica que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Las imágenes captadas por dichos dispositivos serán tratadas únicamente por el Coordinador de Seguridad, que las transmitirá a las Fuerzas y Cuerpos de Seguridad o a las autoridades competentes únicamente en caso de apreciarse en las mismas la existencia de actos o conductas violentas y de actos racistas, xenófobos o intolerantes.

El titular de la instalación será responsable del tratamiento y deberá cumplirse lo dispuesto en el RGPD.

3.4 Entidades financieras

Las entidades financieras como bancos o instituciones de crédito en general, están obligados a adoptar una serie de medidas de seguridad tanto generales como específicas para ejercicio de su actividad.

Entre estas medidas se encuentran la instalación de sistemas de videovigilancia como elemento de prevención ante la comisión de hechos delictivos.

Estas entidades deberán conectar con una central de alarmas propia o ajena los sistemas de seguridad instalados en sus establecimientos y oficinas.

La instalación de este tipo de cámaras y videocámaras es de titularidad privada, siendo las propias entidades las responsables de las mismas.

Las imágenes estarán exclusivamente a disposición de las autoridades judiciales y de las Fuerzas y Cuerpos de Seguridad, a las que se deberán facilitar inmediatamente aquellas que se refieran a la comisión de hechos delictivos.

En principio, las imágenes sólo podrán ser visualizadas por las Fuerzas y Cuerpos de Seguridad, los Jueces y Tribunales, por la Inspección de la Agencia Española de Protección de Datos en el ejercicio de sus competencias, y por el personal legitimado por la Ley de Seguridad Privada.

La respuesta al ejercicio de los derechos de acceso o supresión de los afectados podrá ser denegada por el responsable del tratamiento, debiendo hacerlo de forma motivada. No obstante, el titular de dichos derechos podrá reclamar su caso ante la AEPD.

Las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad.

Se contempla también que las grabaciones deben cancelarse transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes.

No obstante, como ya hemos indicado anteriormente, esta cancelación debe interpretarse en función de lo que el RGPD contempla, que no recoge un derecho de cancelación sino de supresión. Por tanto, ese plazo de quince días, y sin perjuicio de la posible excepción citada en el párrafo anterior, será de supresión. En lo no específicamente previsto por el Reglamento de Seguridad Privada se aplicará el régimen del RGPD.

3.5 Joyerías, platerías, galerías de arte y tiendas de antigüedades

La normativa de Seguridad Privada prevé que –entre otros establecimientos- las joyerías, platerías, galerías de arte y tiendas de antigüedades, puedan disponer de servicios de videovigilancia.

Estos establecimientos deberán informar al público sobre la implantación de estos sistemas de cámaras o videocámaras conforme a la regla general, es decir, mediante la colocación de carteles informativos y disposición de formularios informativos.

En este caso, la obligación de adoptar medidas de seguridad por estas entidades no sustituye las previsiones del RGPD.

La instalación de este tipo de cámaras y videocámaras es de titularidad privada, siendo las propias entidades las responsables de las mismas.

3.6 Grabaciones por detectives privados

La Ley de Seguridad Privada regula, en su artículo 48, la prestación de servicios de investigación privada que pueden ser realizados por detectives privados.

La AEPD considera lícito el tratamiento de datos de carácter personal que puedan derivarse de la realización de actividades de investigación privada, siempre que resulte ajustado a los principios de limitación de la finalidad y minimización y que quede circunscrito al ámbito del encargo en cuyo seno se desarrolla la actividad investigadora, respetando los citados principios y siendo regulada esta actividad mediante la existencia de una relación contractual.

La normativa de seguridad privada actualmente en vigor no legitima cualquier tratamiento de datos por parte de los detectives privados.

Dicho tratamiento queda limitado a la existencia de un interés legítimo que justifique la realización de las tareas de investigación y la garantía de los derechos consagrados en el artículo 18 de la Constitución.

Además de la existencia de interés legítimo, será necesaria la existencia de una relación contractual entre el titular de dicho interés y el detective privado en el marco de las funciones que le reconoce la Ley de Seguridad Privada.

3.7 Comunidades de propietarios, viviendas y otros supuestos

3.7.1- Comunidades de propietarios: zonas comunes

Tratándose de la captación de imágenes en zonas o elementos comunes de comunidades de propietarios, la adopción de esta medida, requiere el acuerdo de la junta de propietarios en los términos previstos en la Ley de Propiedad Horizontal.

Sería conveniente que el acuerdo reflejara las características del sistema de videovigilancia, número de cámaras y espacios que captan.

Cumplido este requisito, la comunidad de propietarios como responsable del tratamiento, estará sujeta a las restantes obligaciones impuestas por la normativa de protección de datos.

Las cámaras sólo podrán captar las zonas comunes de la comunidad, no siendo factible la grabación de imágenes de la vía pública, a excepción de una franja mínima de los accesos al inmueble.

Tampoco se podrá realizar la captación de imágenes de terreros y viviendas colindantes o de cualquier otro espacio ajeno. En este último caso, si se usan cámaras orientables y/o con zoom, será necesaria la instalación de máscaras de privacidad para evitar esta grabación.

Por otra parte, deberá prestarse especial consideración a lo siguiente:

- Se instalarán en los distintos accesos a la zona videovigilada y, en lugar visible, uno o varios carteles que informen de que se accede a una zona videovigilada.

- El cartel indicará de forma clara la existencia del tratamiento, la identidad del responsable, la posibilidad de ejercitar los derechos del artículo 15 a 22 del RGPD y una referencia a dónde obtener más información sobre el tratamiento de los datos personales.
- La AEPD dispone de un modelo de cartel.
- El acceso a las imágenes estará restringido a las personas designadas por la comunidad de propietarios.
- En ningún caso estarán accesibles a los vecinos mediante canal de televisión comunitaria.
- Si el acceso se realiza con conexión a internet, se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por las personas autorizadas a acceder a dichas imágenes.
- Una vez instalado el sistema, se recomienda el cambio regular de la contraseña, evitando las fácilmente deducibles.
- Se pondrá a disposición de los afectados la restante información que exige el artículo 13 del RGPD. La información puede estar disponible en conserjería, recepción, oficinas, tablones de anuncios o ser accesible a través de internet.
- La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a la comunidad del cumplimiento de la legislación de protección de datos.

La instalación de videocámaras en la piscina comunitaria, también se regirá por las reglas anteriormente descritas, puesto que se trata de una zona común de la comunidad de propietarios.

3.7.2 Viviendas unifamiliares

La instalación de sistemas de videovigilancia en viviendas unifamiliares posee unas características especiales:

- Si las cámaras se instalan en el interior de la vivienda se considera que se realiza en el ejercicio de una actividad personal o doméstica, a la que no le es aplicable la legislación de protección de datos.
- Si las cámaras se instalan en el exterior y pueden captar imágenes de personas en entradas, fachadas o medianerías, se aplicarán las previsiones del RGPD en los términos descritos en el apartado anterior.

En este último supuesto, cuando las cámaras se encuentran conectadas a una central de recepción de alarmas dichos servicios sólo podrán prestarse por empresas de seguridad privada que cumplan los requisitos establecidos en la Ley 5/2014, de 4 de abril, ostentando éstas la condición de responsables.

3.7.3 Plazas de garaje

Ya hemos señalado que la captación de imágenes por cámaras de videovigilancia en los espacios comunes de una comunidad de propietarios puede quedar incardinada en la esfera del interés legítimo de dicha comunidad y la finalidad de seguridad es también legítima.

Existirá un interés público de los particulares en la captación de imágenes mediante cámaras de videovigilancia para garantizar la seguridad de personas o instalaciones en los espacios de su propiedad, como puede ser su domicilio o su plaza de garaje.

Respecto a la instalación de cámaras en una plaza de garaje, que a su vez forme parte de un espacio compartido por el que puedan transitar el resto de los propietarios o terceros que acceden al mismo, las imágenes captadas por las cámaras se limitarán exclusivamente a la plaza de aparcamiento de la que sea titular el responsable del sistema de videovigilancia y a una franja mínima de las zonas comunes que no sea posible evitar captar para la vigilancia de la plaza de garaje, previa autorización de la Junta de Propietarios que deberá constar en las actas correspondientes.

Además, no se captarán imágenes de plazas de aparcamiento ajenas ni tampoco de la vía pública, terrenos y viviendas colindantes o de cualquier otro espacio ajeno.

Cumplido este requisito, el propietario de la plaza de garaje como responsable del tratamiento, estará sujeta a las restantes obligaciones impuestas por la normativa de protección de datos.

- Para más información consulte los siguientes informes jurídicos: I y II.

3.7.4 Servidumbres de paso

Si existiese una servidumbre de paso sobre un inmueble o terreno, el propietario podrá también utilizar estos sistemas, siempre que cumplan los principios de proporcionalidad, sobre el terreno cubierto por la servidumbre, aunque por dicho terreno puedan transitar otras personas, entendiendo como tal, a todos aquellos que tienen constituida la servidumbre a su favor y las personas autorizadas.

El tratamiento de los datos no se encontraría excluido del ámbito de aplicación de la normativa de protección de datos, dado que al tratarse de una zona en que está sometida a una servidumbre de paso, resulta accesible no sólo por el titular de la vivienda y las personas autorizadas por este, sino por los terceros titulares del predio dominante de la servidumbre.

En estos casos el tratamiento sería conforme a lo dispuesto en el RGPD cuando tenga por objeto la finalidad legítima de preservación del propio inmueble.

El propietario del inmueble, como responsable del tratamiento, estará sujeto a las restantes obligaciones impuestas por la normativa de protección de datos.

- Para más información consulte este informe jurídico.

3.7.5 Videoporteros

En aquellos casos en los que la utilización de videoporteros se limite a su función de verificar la identidad de la persona que llamó al timbre así como facilitar el acceso a la vivienda, no será de aplicación la normativa sobre protección de datos.

Sin embargo, si el servicio se articula mediante procedimientos que reproducen y/o graban imágenes de modo constante, y en particular cuando el objeto de las mismas alcance al conjunto del patio y/o a la vía pública colindante, o se graben imágenes sobre situaciones que concurran en la portería de un edificio, al exceder estas actuaciones del ámbito personal y doméstico, resultará de plena aplicación el RGPD.

3.7.6 Mirillas digitales

En principio, y al igual que el supuesto descrito anteriormente referido a los videoporteros, el uso de las mirillas digitales estaría excluido en la aplicación de la normativa de protección de datos aplicando la citada excepción doméstica, siempre y cuando su uso se limite a de verificar la identidad de la persona que llamó al timbre y a facilitar el acceso a la vivienda.

Sin embargo, si este tipo de mirillas reproducen y/o graban imágenes, resultará de plena aplicación el RGPD.

3.8 Entornos escolares

La captación de imágenes en entornos como colegios, guarderías, centros lúdicos y espacios similares donde los menores puedan ser objeto de grabación, requiere adoptar ciertas cautelas.

La instalación de cámaras de videovigilancia en estos entornos con el fin de controlar conductas que puedan afectar a la seguridad, sólo será legítima cuando la medida sea proporcional en relación con la infracción que se pretenda evitar y, en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia.

La utilización e instalación de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

Y en todo caso deberán tenerse en cuenta las siguientes indicaciones:

- La zona objeto de videovigilancia será la mínima imprescindible abarcando espacios públicos como accesos o pasillos.
- No podrán instalarse en espacios protegidos por el derecho a la intimidad como baños, vestuarios o aquellos en los que se desarrollen actividades cuya captación pueda afectar a la imagen o a la vida privada como los gimnasios.
- Salvo en circunstancias excepcionales, no podrán utilizarse con fines de control de asistencia escolar.
- Se pueden instalar cámaras en los patios de recreo y comedores cuando la instalación responda a la protección del interés superior del menor, toda vez que, sin perjuicio de otras actuaciones como el control presencial por adultos, se trata de espacios en los que se pueden producir acciones que pongan en riesgo su integridad física, psicológica y emocional.
- La grabación en las aulas mientras los alumnos realizan pruebas de nivel de conocimientos sería desproporcionado.

3.9 Zonas de baño

En el supuesto de las zonas de baño conviene precisar lo siguiente:

- La posibilidad de instalar cámaras en las piscinas de las comunidades propietarios, al ser una zona común, siempre que se adopte de conformidad con lo establecido en la **Ley 49/1960, de 21 de julio**, sobre propiedad horizontal.
- También se pueden instalar en piscinas y spas con fines de garantía de calidad sanitaria y de seguridad de las personas, siempre que se limiten a zonas de uso público y no a espacios reservados como vestuarios o aseos.

Si las cámaras se sitúan en zonas de servicios colectivos, como cafeterías, restaurantes o zonas de pasos, será proporcional su instalación y uso con fines de seguridad.

- Para más información puede consultar este **informe jurídico**.

4. Tratamiento de imágenes con fines diferentes a la seguridad

4.1 Obligaciones generales

En los apartados 2 y 3 de esta Guía hemos analizado el uso de las cámaras con la finalidad de videovigilancia, en relación con la aplicación del contenido del RGPD.

Sin embargo, las cámaras pueden utilizarse para otras finalidades que no están relacionadas con la seguridad, como pueden ser, por ejemplo , el control de la prestación laboral, las grabaciones de sesiones de órganos colegiados, o incluso, la toma de fotos o grabaciones en los eventos escolares.
En el siguiente apartado, se describen algunas de estas situaciones, en las que la finalidad del tratamiento de datos a través de las cámaras no es la seguridad, sino una finalidad diferente.

No obstante, este tipo de tratamientos, aunque la finalidad no sea la seguridad, supone que deben cumplirse las obligaciones y principios del RGPD, atendiendo a las especiales características del citado tratamiento, y en su caso, a la normativa específica que sea de aplicación.

4.2 Tráfico: control y acceso a zonas restringidas

4.2.1 Control de tráfico

La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, y demás normativa específica en la materia, y con sujeción a lo dispuesto en la normativa de protección de datos.

Corresponderá a las Administraciones Públicas con competencia para la regulación del tráfico, autorizar la instalación y uso de estos dispositivos, adoptando una resolución a tal efecto.

La citada resolución, que en el ámbito de la Administración General del Estado será adoptada por la Dirección General de Tráfico:

- Determina la instalación y uso de los dispositivos fijos de captación y reproducción.
- Identifica genéricamente las vías públicas o los tramos de aquellas cuya imagen sea susceptible de ser captada.
- Adopta las medidas tendentes a garantizar la preservación de la disponibilidad, confidencialidad e integridad de las grabaciones o registros obtenidos.
- Especifica el órgano encargado de su custodia y de resolver las solicitudes de acceso y cancelación de los ciudadanos.
- La resolución será indefinida en tanto no varíen las circunstancias que la motivaron.
- Si se utilizan medios móviles de captación y reproducción de imágenes, si bien deberán cumplirse los principios de utilización y conservación referidos, no será necesario la adaptación de esta resolución.
- Para más información consulte el siguiente **informe jurídico**.

4.2.2 Control de acceso a zonas restringidas de tráfico

Relacionado con el punto anterior, se encuentra la utilización de cámaras para controlar el acceso a barrios o calles en las que únicamente pueden acceder aquellos que previamente han sido autorizados.

Este acceso se controla mediante cámaras que captan la matrícula de un vehículo para comprobar si el mismo puede acceder o no a la citada zona, sin que sea necesario captar la imagen de los ocupantes para la finalidad descrita.

4.3 Centros educativos: grabaciones y toma de fotografías en eventos

Respecto a las grabaciones y toma de fotografías de las imágenes de los menores en festivales de navidad, pasacalles o eventos similares, se encontrarán habitualmente encuadrada en el ámbito personal y doméstico y, por tanto, excluido de la aplicación del RGPD, en virtud de lo previsto en su artículo 2.2.c), en la medida en que las imágenes sean tomadas por los padres para sus fines eminentemente familiares. En todo caso, el uso social permite este tipo de grabaciones y realización de fotografías.

Asimismo, esta excepción, y de conformidad con el considerando 18 del RGPD, se aplicaría a la actividad de redes sociales y la actividad en línea siempre y cuando se encuentre vinculada a una actividad personal o doméstica, sin perjuicio de la aplicación de la norma europea a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

Cabe también señalar, que si bien el derecho a la protección de datos puede no resultar de aplicación, sí puede serlo la protección otorgada por otras normas frente a las intromisiones que supongan una vulneración de los derechos al honor, a la intimidad y a la propia imagen, que se regirá por lo dispuesto en la 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, así como la normativa que protege a los menores de edad.

RECUERDE

La AEPD dispone de una sección dedicada a la protección de datos de los menores denominada "Tú decides en Internet".

4.4 Sanidad y centros de asistencia

Sin perjuicio de la instalación de cámaras en centros de salud y hospitales con la finalidad de garantizar la seguridad, la toma y grabaciones de imágenes podrían usarse con la finalidad de asegurar un tratamiento adecuado de la salud, como sería el caso de la monitorización de pacientes en las unidades de vigilancia intensiva, o la telemedicina.

En este supuesto de uso de cámaras con fines sanitarios, en primer lugar, procede la aplicación del RGPD, si bien la legitimación para el tratamiento de los datos, al ostentar los datos de salud la consideración de categorías especiales de datos, la legitimación en este caso vendría dada de la siguiente forma:

- En el primer supuesto, por el artículo 9.2.c) del RGPD, puesto que el tratamiento es necesario para proteger los intereses vitales del afectado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente para dar su consentimiento.
- En el segundo supuesto, por el artículo 9.2.h) del RGPD ya que el tratamiento es necesario para fines de medicina preventiva, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario sobre la base del Derecho de la Unión Europea o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3 del citado artículo 9.

Aunque la finalidad sea la videovigilancia, se considera desproporcionado el uso de cámaras en las habitaciones de los pacientes para que sus familiares puedan visionar en “streaming” su estado de salud.

4.5 Investigación científica y usos afines

Uno de los fines posibles para la captación y grabación de imágenes relativos a personas identificadas o identificables son la investigación, ya se trate de investigación científica, del estudio de hábitos de uso o consumo, o incluso en el ámbito de los procesos de selección de personal.

Por tanto, en este caso se aplicarán plenamente las previsiones del RGPD. En este sentido, debe recordarse la especial importancia que reviste en esta materia el cumplimiento de los principios de limitación de la finalidad y minimización en el tratamiento de los datos.

En todo caso, el RGPD dedica un artículo específico, el 89, al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, indicando que estará sujeto a las garantías adecuadas para los derechos y libertades de los interesados, disponiendo de medidas técnicas y organizativas, en particular para garantizar el principio de miminización de los datos personales, pudiendo incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines.

4.6 Grabaciones de órganos colegiados de las AAPP y asambleas

En el ámbito de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha previsto que se puedan graban las reuniones que celebren los órganos colegiados, pudiendo el fichero resultante de la grabación acompañar al acta de las sesiones. Estas grabaciones deberán conservarse de forma que se garantice la integridad y autenticidad del citado fichero, así como el acceso al mismo por parte de los miembros del órgano colegiado.

Esta grabación de las sesiones podría incluirse en la regulación de funcionamiento del respectivo órgano colegiado, o a través de un instrumento como su reglamento de régimen interior. Asimismo, también podría preverse si la grabación se va a utilizar como ayuda para la elaboración del acta, o va a formar parte de la misma como un anexo.

Por lo que se refiere a las grabaciones de asambleas (por ejemplo, en asociaciones, comunidades de propietarios o sociedades mercantiles), la grabación se legitimaría por el artículo 6.1.f) del RGPD en base al interés legítimo.

5. Tratamiento de imágenes a través de tecnologías emergentes

5.1 Cámaras "on board"

Este tipo de tecnología consiste en instalar una cámara dentro de un vehículo o también en ocasiones en el casco del conductor, e ir grabando todo el recorrido que se realiza con el mismo. Incluso, existen vehículos que ya llevan incluidos este tipo de cámaras.

Sobre este tipo de grabaciones procede distinguir dos tipos de supuestos:

- Las grabaciones para una finalidad "doméstica", que estaría exceptuada de la aplicación de la normativa de protección de datos. Por ejemplo, el uso de estas cámaras en los cascos de un ciclista o motorista, que fuesen tomando imágenes paisajísticas.

  No obstante, su uso posterior, como por ejemplo, la publicación de las grabaciones en internet quedaría sometido a la normativa de protección de datos.

- Las grabaciones con la finalidad de obtener pruebas para determinar responsabilidades asociadas a la producción de un suceso, es decir, obtener fotografías o grabaciones de imágenes como pruebas en relación con posibles accidentes o incidencias de tráfico.

  Este segundo tipo de grabaciones vendrían permitidas por la aplicación de la regla del interés legítimo (art.6.1.f del RGPD), en base al derecho a la tutela judicial efectiva, derecho fundamental recogido por la Constitución Española de 1978.

  No obstante, el hecho de que se puedan realizar las grabaciones, no es óbice para la adopción de una serie de cautelas, como podría ser que la grabación únicamente se active en caso de producirse un suceso concreto, o bien la activación manual, o atendiendo al principio de minimización, que la imágenes que se capten hacia el exterior queden limitadas al frontal del vehículo. Para más información puede consultar este informe judírico.

5.2 Drones

Otra de las tecnologías que junto a las cámaras "on-board" se han popularizado en los últimos años son las aeronaves pilotadas de forma remota, más conocidas con el nombre de drones.
Los drones pueden llevar o no, sistemas de procesamiento de información (de datos en general) de muy diversos tipos: sistemas de grabación de imagen, sistemas de detección (sensores ópticos o electrónicos, infrarrojos, de humos), o equipos de radiofrecuencia (antenas para capturar emisiones de radio o de wi-fi). En este sentido, y a los efectos de la finalidad de esta Guía, nos vamos a referir a la posible captación y procesamiento de imágenes de los drones, a través de las cámaras que lleven incorporadas.

En muchas ocasiones, el interesado o afectado desconocerá la misma existencia del dron o del tratamiento de imágenes que se está realizando, ya que puede recoger datos sin ser visto por las personas y sin estar sujeto a barreras físicas concretas para desplazarse.

El Grupo de Trabajo del artículo 29, del que forma parte la AEPD, analizó este tipo de grabaciones utilizando drones en el Dictamen 01/2015, de 16 de junio de 2015, por lo que teniendo en consideración dicho Dictamen, y de forma resumida debe tenerse en cuenta lo siguiente:

- La operativa del dron habrá de cumplir con la normativa aplicable
- Valorar la posibilidad de realizar una Evaluación de Impacto de la Protección de Datos, atendiendo al tipo de dron y la tecnología de captación de datos para el tratamiento
- Evitar captar o tratar datos innecesarios a la finalidad pretendida
- Informar de la forma más apropiada y con carácter previo a los afectados, incluyendo una indicación clara de quién es el responsable y las finalidades del tratamiento, así como las indicaciones claras y específicas para el ejercicio de derechos
- Establecer medidas de seguridad apropiadas para los riesgos que representan el tratamiento pretendido
- Borrar y/o anonimizar cualquier dato innecesario
- Para más información puede consultar este **informe judírico**.

6. Supuestos de no aplicación de la normativa de protección de datos

6.1 Tratamiento de imágenes en el ámbito personal y doméstico

El RGPD no se aplica al tratamiento de imágenes efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Anteriormente, ya nos hemos referido a dos supuestos concretos, como serían los videoporteros y las mirillas digitales, siempre y cuando no reproduzca y/o graben imágenes.

Sobre la aplicación de esta excepción doméstica, no podrán entenderse exceptuados aquellos supuestos en los que la información tratada sea puesta en conocimiento de un número indeterminado o indefinido de personas.

Si un usuario de redes sociales actúa en nombre de una empresa o de una asociación o lo utiliza como una plataforma con fines comerciales, políticos o sociales, la excepción de ámbito personal o doméstico no se aplica.
Tampoco se aplica la excepción en aquellos casos en los que el tratamiento de estos datos pueda lesionar los derechos e intereses de las personas. A tal efecto, debe tenerse en cuenta que la utilización de las tecnologías de la información y las comunicaciones puede dar lugar a que un tratamiento de los datos inicialmente vinculado con la vida privada de quien lo realiza pueda implicar un acceso a información de un tercero que éste no desea que sea del dominio público.

6.2 Tratamiento de imágenes por los medios de comunicación

La publicación de imágenes en los medios de comunicación supone un ejercicio del derecho a la libertad de expresión e información que les confiere el artículo 20 de la Constitución Española.

En el supuesto de que algún particular considerase lesionado sus derechos por la publicación de imágenes, tendría que acudir a la vía judicial al amparo de lo dispuesto en la Ley Orgánica 1/1982, de 5 mayo.

En todo caso, el RGPD contiene un mandato a los Estados miembros para que concilien por ley el derecho a la protección de datos de la norma europea con el derecho a la libertad de expresión y de información, incluyendo el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

6.3 Uso de cámaras simuladas

El RGPD se aplica cuando se produce un tratamiento de los datos personales de personas físicas.

En el caso de cámaras simuladas este tratamiento no existe, por lo que no cabe aplicar la citada norma, partiendo de la imposibilidad material de puesta en funcionamiento de las cámaras, por carecer de todos los elementos técnicos que fueran necesarios para su utilización.

No obstante lo anterior, conviene precisar lo siguiente:

Si se tratara de cámaras reales desactivadas o que pueden ser activadas sin esfuerzos excesivos, deberán aplicarse los principios vigentes en materia de protección de datos personales y la normativa sectorial que resulte de aplicación.

6.4 Promoción turística y finalidades relacionadas

La difusión de imágenes con finalidad promocional a través de internet es una práctica cada vez más común, ya se trate de difundir un determinado ámbito corporativo -como fachadas de edificios o espacios singulares en empresas o instituciones-, ya se refiera a lugares de interés turístico. Únicamente cuando la captación y emisión de las imágenes no afecte a personas identificadas o identificables resultará excluida la aplicación del RGPD.

No sería de aplicación el RGPD cuando las imágenes muestren una panorámica general de una playa en la que no sea posible la identificación de las personas, como sería el caso cuando el objetivo de las imágenes fuera mostrar el estado del oleaje para proporcionar información a los aficionados del surf acerca de las condiciones para la práctica de este deporte.

- Para más información sobre uso de videocámaras para fines de promocionar el turismo y captación de imágenes panorámicas, consulte este informe jurídico.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

www.aepd.es