***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

26/3/2021

Trabajo 2

Toma de Datos de Zonas Publicas

Diseño y Administración de Sistemas y Redes

Contenido

[1. Protección de Datos 3](#_Toc66386410)

[1.1. ¿Qué es la Protección de Datos? 3](#_Toc66386411)

[1.2. ¿Qué entendemos por datos personales? 3](#_Toc66386412)

[1.2.1. Tipos de datos personales 4](#_Toc66386413)

[2. Historia de la Protección de Datos 5](#_Toc66386414)

[2.1. Edad antigua: Grecia y Roma 5](#_Toc66386415)

[2.2. Edad Media 5](#_Toc66386416)

[2.3. Edad Moderna: La razón 5](#_Toc66386417)

[2.4. Protección de Datos en España 6](#_Toc66386418)

[2.4.1. Previa a la Constitución del 78 6](#_Toc66386419)

[2.4.2. Posterior a la Constitución del 78 6](#_Toc66386420)

[3. LOTARD y LOPD 7](#_Toc66386421)

[3.1. LORTARD 7](#_Toc66386422)

[3.2. LOPD 7](#_Toc66386423)

[3.2.1. Titulo 1: Ley LOPD 7](#_Toc66386424)

[3.2.2. Titulo 2: Principios 7](#_Toc66386425)

[3.2.3. Titulo 3: Derechos de las personas 8](#_Toc66386426)

[3.2.4. Titulo 4: Disposiciones sectoriales 8](#_Toc66386427)

[3.2.5 Titulo 5: Movimiento internacional de datos 8](#_Toc66386428)

[3.2.6. Titulo 6: Órgano de Control 9](#_Toc66386429)

[3.2.7. Titulo 7: Infracciones y sanciones 9](#_Toc66386430)

[4. Asociación Española De Protección de Datos 10](#_Toc66386431)

[4.1 ¿Que es la AEPD? 10](#_Toc66386432)

[4.2 Derechos 11](#_Toc66386433)

[4.2.1. Derecho de acceso 11](#_Toc66386434)

[4.2.2. Derecho de rectificación 11](#_Toc66386435)

[4.2.3. Derecho de Oposición 11](#_Toc66386436)

[4.2.4. Derecho de supresión (“al olvido”) 11](#_Toc66386437)

[4.2.5. Derecho a la limitación del tratamiento 12](#_Toc66386438)

[4.2.6. Derecho a la portabilidad 12](#_Toc66386439)

[4.2.7. Derecho a no ser objeto de decisiones individuales automatizadas 12](#_Toc66386440)

[4.2.8. Derecho de Información 12](#_Toc66386441)

[4.2.9. Derechos Schengen 13](#_Toc66386442)

[4.3. Deberes 13](#_Toc66386443)

[4.3.1. Ejemplos de Medidas de Cumplimiento 13](#_Toc66386444)

[4.3. Donde y como actúa la AEPD 17](#_Toc66386445)

[4.3.1. Internet y redes Sociales 17](#_Toc66386446)

[4.3.2. Publicidad no deseada 17](#_Toc66386447)

[4.3.3. Violencia de género y violencia digital 18](#_Toc66386448)

[4.3.4. Protección de datos y Coronavirus 19](#_Toc66386449)

[4.3.5. Educación y menores 19](#_Toc66386450)

[4.3.6. Videovigilancia 19](#_Toc66386451)

[4.4. Herramientas que proporciona la AEPD 20](#_Toc66386452)

[4.4.1. Facilita RGPD 20](#_Toc66386453)

[4.4.2. Canal del Delegado de Protección de Datos 20](#_Toc66386454)

[4.4.3. Gestiona EIPD 20](#_Toc66386455)

[4.4.4. Facilita Emprende 21](#_Toc66386456)

[4.4.5. Comunica-Brecha RGPD 21](#_Toc66386457)

[5. Ejemplos de sentencias 22](#_Toc66386458)

[5.1. Multa a la Mutua Madrileña (Procedimiento nº.: PS/00586/2017) 22](#_Toc66386459)

# Introducción

## 1.1. Esquema del trabajo

En este apartado veremos como se organizará el trabajo, para una mejor comprensión de este.

En primer lugar, veremos las diferentes leyes que tienen que ver con el tema de la videovigilancia, tanto en España como en otros países, para tener una comparativa general.

Posteriormente, veremos, ya centrados en España, casos mas concretos, como la toma de videos por parte de la policía o la dgt, con ejemplos de como realizan esta videovigilancia, y las leyes que los amparan.

Después hablaremos de casos curiosos relacionados con el tema de la videovigilancia; y por último, pondremos algunos ejemplos de denuncias y fallos, y las comentaremos.

## 1.2. ¿A que nos referimos con toma de datos en zonas públicas?

En este trabajo, nos referimos a toma de datos en zonas públicas, a los datos recopilados por particulares, empresas o instituciones.

En concreto, nos centraremos en la toma de videos, tanto de cámaras de videovigilancia, como de videos realizados por particulares.

# Legislación

## 2.1. Legislación en España

La ley que legisla actualmente este tema en España es la Ley Orgánica de Protección de Datos, redactada en 1999 y revisada en 2018, para concretar la garantía de los derechos digitales. Esta ley consta de 7 títulos principales, pero los que nos interesan son principalmente el Titulo 1, el Titulo 2 y el Titulo 3.

### 2.1.1. Titulo 1: Introducción

El **objetivo** de este título es **garantizar y proteger el tratamiento de datos personales**, y se aplica a los datos de carácter personal registrados en soporte físico susceptibles de tratamiento y uso posterior por los sectores público y privado.

Sin embargo, hay algunos **ficheros regulados según legislación específica**, como ficheros con fines estadísticos (Legislación del régimen electoral), ficheros de informes de calificación del régimen personal de las fuerzas armadas, ficheros del registro civil y del registro de penados y rebeldes, y de imágenes y sonidos de videocámaras de las fuerzas y cuerpos de seguridad.

Como podemos observar, aquí empezamos a ver que las imágenes y sonidos de videocámaras de fuerzas de seguridad tienen una legislación aparte, que cubriremos más adelante.

### 2.1.2. Titulo 2: Principios

* **La calidad de los datos:** Exactitud, puesta al día, pertinencia, posibilidad de utilización, almacenamiento.
* **El derecho de información** al dueño de los datos de la existencia del fichero, derecho al acceso de datos, conocimiento de los datos y a exigir cancelación o rectificación.
* **El principio de consentimiento**

De este titulo nos interesa sobre todo el **principio de consentimiento**, ya que, muchas veces en la grabación de video en las zonas públicas, las personas no saben que están siendo grabadas. Por lo tanto, una primera impresión que nos da es que, si a una persona la graban por la calle, tiene todo el derecho a solicitar que se elimine ese video, y con esto enlazamos con el tercer título. Sin embargo, mas adelante veremos casos en los que esto no es así.

### 2.1.3. Titulo 3: Derechos de las personas

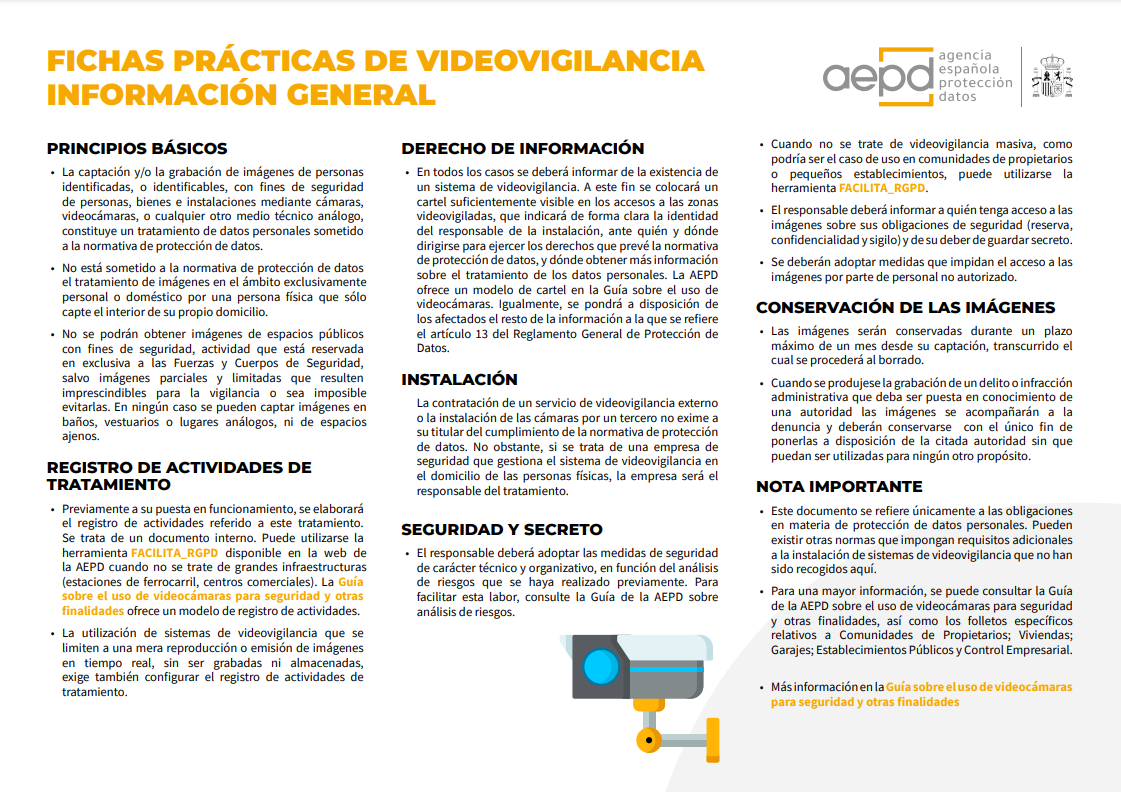
En este titulo vemos los derechos que pueden ejercer las personas sobre los datos que han tomado sobre ellas (en nuestro caso, los videos que se les han grabado). Como bien decíamos en los anteriores puntos, esto puede variar dependiendo el origen de la grabación, y lo concretaremos más adelante.

* **Derecho de Impugnación**: Los ciudadanos tienen derecho a no verse sometidos en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. Podrán impugnar un tratamiento de datos que ofrezca una definición de sus características o personalidad.
* **Derecho información y acceso del afectado** respecto a sus datos de carácter personal (más de 12 meses).
* **Derecho de rectificación y cancelación**: datos inexactos, incompletos o no adecuados. (10díashábiles)
* **Indemnización**: Cuando sufra daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en esta Ley.

### 2.1.4. AEPD

En la agencia Española de protección de datos, se nos brinda ayuda a los particulares que quieran colocar cámaras de seguridad, pero que no conozcan muy bien la legislación.

Si nos vamos a su [pagina web](https://www.aepd.es/), al apartado “Áreas de Actuación”, y dentro de este, a “Videovigilancia”, tenemos guías muy practicas sobre cuando podemos poner y cuando no cámaras de seguridad. A continuación veremos el folleto con información general, y resumiremos los diferentes apartados que exponen.



#### Cámaras en una vivienda

Habrá que tener en cuenta la normativa cuando la captación de imágenes pueda incluir a personas en el exterior de la vivienda.

Primero tenemos que elaborar un registro, para el que la AEPD nos proporciona la herramienta **facilita\_rgpd**. Posteriormente, tenemos que ejercer el derecho a la información: **informar a todas las personas que puedan ser grabadas la existencia de un sistema de videovigilancia**.

La instalación será **solo en la vivienda** de la que se es titular, y **no podrán tomarse imágenes de la vía publica** (excepto si es una pequeña franja de los accesos a la vivienda). Si la cámara es orientable o con zoom, se tendrán que instalar **mascaras de privacidad**. El **responsable** de cumplir estas normas es el **titular** del domicilio, no la empresa que monte el sistema de videovigilancia.

El **acceso a las imágenes será exclusivo del responsable**, y si se realiza a través de internet, será mediante un usuario y una contraseña, o cualquier otra manera de autentificación.

Las imágenes se mantendrán durante un **máximo de un mes**.

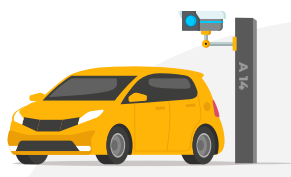
#### Cámaras en plazas de garaje

Esta normativa se aplicará cuando el garaje forme parte de un espacio compartido por el que puedan transitar el resto de los propietarios o terceros.

Al igual que en el resto de las instalaciones, se elaborará el **registro de actividad propio** referido a este tratamiento (puede ser con la aplicación facilita\_rgpd). Este es un documento interno.

Asimismo, también tendremos que ejercer el **derecho de información**, informando a todas las personas que puedan ser grabadas de que existe un sistema de videovigilancia. Esto se podrá hacer mediante carteles en las zonas vigiladas, en el que pondrá la identidad de quien realiza la grabación, y donde dirigirse para ejercer sus derechos.

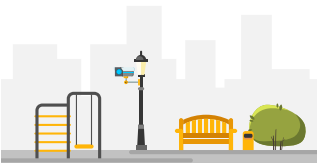
La **grabación se limitará solo a la plaza de garaje**, y si es necesario, a una pequeña franja de las zonas comunes que no sea posible evitar para la vigilancia de la plaza. Esta vigilancia tiene que ser **aprobada por la junta de propietarios**. No podrán captarse imágenes de la vía publica, terrenos u otras viviendas, y de usar cámaras orientables, habrá que instalar una mascará de privacidad para evitar esto.

El acceso a las imágenes será exclusivo del responsable, y si se realiza a través de internet, será mediante un usuario y una contraseña, o cualquier otra manera de autentificación.

El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido, y las imágenes se mantendrán durante un **máximo de un mes**.

#### Comunidades de propietarios

Primero, para la instalación de cámaras, se debe haber **aprobado en junta de Propietarios.**

A la hora de colocarlas, se debe **ejercer el derecho de información**, colocando carteles que informan que se accede a una zona videovigilada. A la hora de la instalación, las cámaras solo podrán captar **imágenes de las zonas comunes** de la comunidad, **nunca de la vía pública**, salvo que resulte necesario para la finalidad perseguida.

El **acceso** a las imágenes está **restringido a las personas designadas por la comunidad**. Las imágenes se conservarán como máximo un mes.

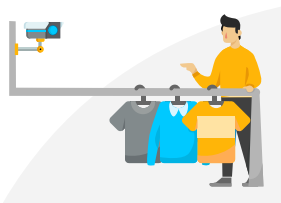
#### Establecimientos públicos

Esta información es solo para la vigilancia del establecimiento por razones de seguridad. Si lo que queremos es vigilar a los trabajadores, veremos las directrices en el siguiente punto.

El primer paso que hay que hacer es, como en toda instalación que vamos viendo, elaborar el **registro de actividad propio** referido a este tratamiento (puede ser con la aplicación facilita\_rgpd). Este es un documento interno.

Como mínimo tiene que haber **un cartel en un lugar visible** informado de que la zona está siendo videovigilada.

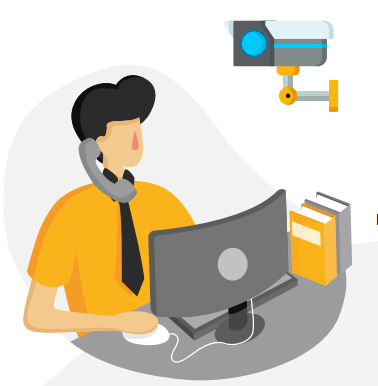
Las imágenes captadas por las cámaras se limitarán al establecimiento público de que se trate, salvo que sea imprescindible para la finalidad perseguida. En el caso de cámaras orientables, igual que en los casos anteriores, tendremos que instalar máscaras de privacidad.

El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes solo podrá acceder el responsable del sistema, autentificándose de la manera oportuna si es vía internet, y se mantendrán durante un **máximo de un mes**.

#### Control laboral

El Estatuto de los Trabajadores da la posibilidad al empresario para adoptar las **medidas que estime más oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales**, que deberán guardar la consideración debida a la dignidad humana y tener en cuenta la capacidad real de los trabajadores con discapacidad.

Solo se debe recurrir a videovigilancia para control empresarial sea **proporcional** el modo en el que se traten las imágenes y la finalidad perseguida, y no haya otra medida más idónea. También se deberá tener en cuenta el **derecho a la intimidad** y a la **propia imagen** de los trabajadores.

Los **trabajadores deberán ser informados** en todo momento de que están siendo grabados, principalmente con un cartel, para el cual podemos usar un modelo de cartel que nos proporciona la Agencia Española de Protección de Datos.

Las cámaras sólo para el control laboral. En ningún caso se ubicarán en zonas de vestuarios, baños y espacios de descanso de los trabajadores.

El acceso a las imágenes será exclusivo del responsable, y si se realiza a través de internet, será mediante un usuario y una contraseña, o cualquier otra manera de autentificación.

El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido, y las imágenes se mantendrán durante un **máximo de un mes**.

## 2.2. Legislación en estados Unidos

En los Estados Unidos de América, las leyes para la videovigilancia, a mi parecer, dejan bastante que desear. El único tratado firmado para todos los estados es el **USA PATRIOT Act**, ya que no hay ninguna ley federal firmada con respecto a la videovigilancia, por lo que cada estado ha de crear sus propias leyes estatales para tratar este tema. A continuación explicaremos por encima el tratado PATRIOT, y las diferentes legislaciones que hay en los estados.

### 2.2.1. USA PATRIOT Act

El USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Es un acto del congreso de los estados unidos cuyo propósito es, como su propio nombre indica, proveer a la nación herramientas útiles para interceptar y obstruir el terrorismo.

Fue firmado a raíz de los atentados del 11 de Septiembre, y una de sus cláusulas principales es expandir las libertades para las cámaras de videovigilancia, así como para “pinchar” teléfonos, tanto nacionales como internacionales.

El título que nos interesa es el **Title 2: Scope of allowed surveillance**, en el que habla de los cambios producidos en todo el tema de las cámaras de seguridad. Lo que principalmente nos dice, es que se pueden utilizar cámaras de seguridad mientras que no violen la primera enmienda (No se les pueden prohibir a los ciudadanos su derecho a la libertad de expresión, de religión o de reunión), y que las autoridades tienen muchas más facilidades para acceder a estas cámaras.

### 2.2.2. Leyes estatales

En este apartado, se clasificarán los diferentes estados conforme a las leyes que tienen en el tema, y se explicará un poco en qué consisten.

#### New Hampshire, Maine, Kansas, South Dakota y Delaware

En estos estados, los establecimientos necesitan un consentimiento para instalar una cámara oculta de cualquier tipo.

#### Tennessee, Michigan, and Utah

En estos estados no necesitas **ningún tipo de permiso** para instalar cámaras de seguridad en sitios públicos, pero si que lo necesitas para colocar cámaras ocultas en lugares considerados privados.

#### Hawaii

Las leyes estatales de Hawaii dicen que si quieres instalar una cámara de seguridad en Hawaii, debes tener el consentimiento de a quienes vas a grabar.

#### Florida, Alabama y Minnesota

En estos estados, es **legal la videovigilancia oculta**, siempre que no sea en lugares no privados. Entendemos estos lugares como los lugares en los que una persona puede esperar un cierto grado de privacidad (Baños, vestuarios, duchas, habitaciones, etc.).

#### California

En California es **ilegal hacer videos grabando conversaciones** que son consideradas confidenciales. Entienden que esta información es pasada de un individuo a otro, y la intención es que solo la escuche el receptor.

#### Arkansas

Las leyes estatales en Arkansas dicen que se pueden grabar a personas en lugares privados, pero con su consentimiento

#### Georgia

En Georgia se permiten las cámaras de vigilancia tanto en lugares públicos como privados, siempre y cuando se vean a simple vista.

#### Otros estados

En el resto de los estados no hay leyes específicas para este tema, pero eso no significa que se puedan instalar cámaras de vigilancia sin ningún tipo de cuidado.

Que no haya leyes quiere decir que un juez no tiene ninguna regla para seguir a la hora de sentenciar un caso, y esto puede jugar en favor o en contra del dueño de las cámaras de vigilancia.

# 3. Toma de videos en lugares públicos en España

En este apartado, se hablará de diferentes casos en los que se toman imágenes en la vía publica, que leyes (de las que hemos comentado, u otras nuevas) les ampara y ejemplos de ello.

## 3.1. Policías y cuerpos del estado

En cuanto a las fuerzas del estado, tienen una legislación propia para el tema de la videovigilancia, que 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 en lugares públicos. Esta ley esta pensada para asegurar la convivencia ciudadana, la erradicación de la violencia, y el tratado de las grabaciones para la prevención de delitos.

### 3.1.1. Cámaras fijas

Para instalar una cámara fija, las fuerzas del estado han de avisar previamente a un órgano colegiado (articulo 1.2). Posteriormente, será autorizado por el Delegado del Gobierno en la Comunidad Autónoma, después de que una comisión, presidida por el Presidente del Tribunal superior de justicia. Se tendrá en cuenta si se instalan para asegurar protección de edificios públicos y su acceso, salvaguardar instalaciones de defensa nacional, constatar infracciones a la seguridad ciudadana, y prevenir daños.

Cuando se acepte la instalación de la cámara, **se acordarán también todas las limitaciones de esta.** Pueden ser la prohibición de grabar audio (excepto si es estrictamente necesario), la precisión del lugar donde se va a grabar, y la duración de la autorización.

### 3.1.2. Cámaras móviles

Los criterios **son semejantes a los de las cámaras fijas**, pero con la diferencia de que, si hay mucha urgencia en obtener las imágenes, y no hay tiempo de pedir la orden, se podrán tomar imágenes sin tener la orden y, en un plazo de 72 horas, informar al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión. Si estos organismos emiten un informe negativo, se destruirán todas las grabaciones realizadas.

Otra diferencia es que hay que renovar la licencia cada 15 días, a diferencia del año de autorización que tienen las cámaras fijas.

### 3.1.3. Derechos del público y sanciones

El público siempre tendrá que **ser informado de forma clara** de que esta siendo grabado, y toda persona interesada puede ejercer los derechos de acceso y **cancelación de las grabaciones** en las que figura. Sin embargo, estos derechos podrán ser denegados, en función del peligro que esto pueda derivar para la seguridad pública y privada, o las necesidades de investigaciones que se estén realizando.

Las infracciones son las mismas que en la Ley Orgánica de Protección de Datos.

## 3.2. Radares de circulación

He incluido este apartado, porque me parece que la toma de fotos de la matricula de nuestro coche también se puede considerar videovigilancia en zona publica, ya que están grabando algo que es una propiedad privada, como es nuestro coche.

La instalación de estas cámaras y radares los ampara el **Articulo 68 del Reglamento de Circulación**, que nos dice que **Los agentes de la autoridad** responsable de la vigilancia, regulación y control del tráfico **podrán utilizar o situar sus vehículos en la parte de la vía que resulte necesaria** cuando presten auxilio a los usuarios de esta o **lo requieran las necesidades del servicio** o de la circulación. Asimismo, determinarán en cada caso concreto los lugares donde deben situarse los vehículos de servicios de urgencia o de otros servicios especiales.

Como podemos observar, no limita mucho los lugares en los que los agentes pueden poner radares.

Sin embargo, un dato curioso a tener en cuenta es que según la **orden ITC/3123/2010**, se hace referencia al “mantenimiento” que tienen que tener los radares con respecto al clima. En el Anexo III recoge textualmente que “salvo que el instrumento sea capaz de detectar, seguir e identificar inequívocamente el objetivo durante todo el proceso de medición, a los instrumentos instalados de forma fija y diseñados para operar bajo circunstancias donde no es posible la presencia continua del operador que vigile sus especificaciones de funcionamiento, ***se les exigirá al menos dos fotogramas del vehículo infractor tomados en diferentes instantes***: uno de ellos mostrará una ***visión panorámica del vehículo***; el otro, su ***placa de identificación***”.

Esto es una forma de concretar la veracidad de las grabaciones, como ejemplo de aplicación del principio de consentimiento para la recogida de los datos de la LOPD.

# 4. Ejemplos de acceso a videos en zonas publicas

En este apartado veremos que, pese a todo lo comentado con anterioridad sobre la toma de datos, hay cosas que aun legales, son éticamente cuestionables.

Dividiremos este apartado en dos, refiriéndonos a España y a otros países, y veremos como podemos acceder de forma fácil y legal a grabaciones de la vía pública.

Antes de nada, hay que tener en cuenta que para acceder a una cámara de seguridad, necesitamos 3 cosas:

* Estar en su **misma red**
* Conocer la **dirección de la cámara** dentro de esta red
* Conocer el **usuario o contraseña** (si las hubiera), para acceder a su contenido.

En este apartado nos aprovecharemos de que muchas cámaras de seguridad están conectadas a internet y no a redes privadas cerradas, sus direcciones ip son públicas, y en muchas ocasiones no hace falta ni usuario ni contraseña.

4.1. España

Como bien hemos mencionado en el apartado anterior, nos aprovecharemos de las