Universitat Oberta de Catalunya

uoc.edu

La videovigilancia con reconocimiento facial en España tras la RGPD.

Pablo Nieto Sacristán
Máster Universitario en Seguridad de las TIC.
Aspectos legales de la seguridad informática.

Josep Cañabate Pérez
Montse Serra Vizern

19/12/2019

B) GNU Free Documentation License (GNU FDL)

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*La videovigilancia con reconocimiento facial en España tras la RGPD.*
Nombre del autor:	*Pablo Nieto Sacristán*
Nombre del consultor/a:	*Josep Cañabate Pérez*
Nombre del PRA:	*Montse Serra Vizern*
Fecha de entrega (mm/aaaa):	12/2019
Titulación:	*Máster Universitario en Seguridad de las TIC.*
Área del Trabajo Final:	*Aspectos legales de la seguridad informática.*
Idioma del trabajo:	*Español*
Palabras clave	*RGPD, videovigilancia, reconocimiento facial, privacidad.*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

En este trabajo de fin de grado se ha estudiado la situación de España en lo relativo a la normativa que regula la videovigilancia y el impacto de la RGPD sobre la misma, haciendo especial foco en cómo afecta este conjunto de normas y leyes al uso de las nuevas tecnologías de reconocimiento facial junto con cámaras de videovigilancia y el impacto que tienen sobre la privacidad. Para ello se ha analizado el contexto histórico reciente en materia de seguridad y privacidad, así como el impacto que ha tenido el avance de la tecnología en este tema. Por otro lado, se ha analizado la legislación en España en materia de videovigilancia, para finalmente estudiar el impacto sobre la seguridad y la privacidad del uso del reconocimiento facial junto con cámaras de videovigilancia, y las distintas soluciones que a este conflicto se están dando en diversos países incluido España.

Abstract (in English, 250 words or less):

In this master's Thesis, I have research about the current situation in Spain regarding the regulations governing video surveillance and the impact of the RGPD on them, focusing on how this set of rules and laws affects the use of new facial recognition technologies together with video surveillance cameras and the impact that they have on privacy. For this, I have studied the recent historical context in the area of security and privacy, as well as the impact that the latest advances in technology has had on this issue. On the other hand, I have analysed the legislation in Spain on video surveillance in order to study the impact on security and privacy of the use of facial recognition along with video surveillance cameras, and the different solutions that various countries, including Spain, has given to this conflict.

Índice

1. Introducción

1.1 Contexto y justificación del Trabajo

Con la entrada en vigor del Reglamento General de Protección de Datos (RGPD) [1], se ha hecho necesario una profunda revisión de la forma de tratar datos de carácter personal, para adecuarse a la nueva normativa.

Este nuevo reglamento, trae consigo cambios profundos en la forma en la que hasta ahora se garantizaba la protección de los datos de carácter personal en toda la unión europea incluida España. Así pues, mientras distintos organismos, como la Agencia española de protección de datos, publican distintas ayudas y documentos para ayudar a particulares y empresas a comprender cuáles son sus nuevos derechos y obligaciones con este nuevo reglamento, se hace también necesario un análisis paralelo de distintas cuestiones que si bien no parecen por el momento no han recibido una gran atención, son sin duda, cuestiones que tarde o temprano deberán ser analizadas y respondidas. Una de ellas es sin duda, el tratamiento de datos e imágenes para investigación de delitos relacionados con terrorismo.

Con el miedo al terrorismo que surgió tras los atentados del 11 de Septiembre en EEUU a escala global, y tras el refuerzo que tuvo este miedo por parte de los propios estados, que utilizaron este atentado y otros posteriores para lanzarse a una recopilación de datos masiva de sus propios ciudadanos con la excusa de la prevención de ataques terroristas, se ha llegado a un punto en el que la lucha por el derecho a la privacidad en la que se engloba la protección de datos personales, choca de forma directa con los esfuerzos de los estados por prevenir nuevos ataques terroristas.

Este problema, lejos de irse solucionando con el paso de los años, se ha visto agravado por el espectacular avance que está desarrollando la tecnología en las últimas décadas. Así, los ciudadanos hemos pasado, por ejemplo, a vivir en ciudades cada vez más monitorizadas que ya incluso en algunas partes de países como China son capaces de efectuar un reconocimiento facial e identificar a delincuentes y gente con antecedentes.

España no es una excepción a todos estos problemas, y si bien el nuevo reglamento parece bastante garantista a la hora de proteger los datos personales, el conflicto entre seguridad y privacidad está lejos de quedar resuelto y se hace necesario un análisis que permita ver cuál es la tendencia actual en España ante este conflicto de la seguridad y la privacidad en lo relativo a nuevas tecnologías y nuevos usos de algunas antiguas, lo cual analizado junto a la tendencia a este mismo respecto en el resto del mundo podrá permitirnos predecir hacia donde podría

inclinarse la balance nuestro país en este choque entre la seguridad y la privacidad.

1.2 Objetivos del Trabajo

El presente trabajo pretende analizar el presente y futuro del tratamiento de imágenes para investigaciones en posibles delitos de terrorismo bajo el nuevo reglamento general de protección de datos implantado por la unión europea desde un punto de vista del equilibrio entre la privacidad y la seguridad. Adicionalmente, y como no podría ser de otro modo, se desprenderán resultados no solo aplicables al tratamiento de imágenes si no para otros tipos de datos de carácter personal susceptibles de ser usados en investigaciones de este tipo.

1.3 Enfoque y método seguido

La metodología escogida para la realización de este trabajo consiste en realizar primero un análisis de cómo ha evolucionado el conflicto entre la seguridad y la privacidad y de las causas que han lo han provocado, haciendo especial énfasis en cómo la tecnología ha afectado y afectará en el futuro a nuestra privacidad, haciendo nuevamente una mención especial a la videovigilancia y sistemas de reconocimiento facial. Posteriormente, se analiza la actual legislación española en materia de videovigilancia y se estudia la influencia de la RGPD en esta materia. Una vez hecho esto, se pasa al estudio del caso del reconocimiento facial en cámaras de videovigilancia y la solución que se le ha dado en distintos países, para terminar con el análisis de este caso en España.

Esta metodología resulta especialmente interesante ya que permite ver en primer lugar la tendencia de los últimos años respecto a la evolución de la privacidad y, además, permite analizar con perspectiva los avances y retrocesos en esta materia, haciéndonos de esta forma una idea de cual podría ser el camino a seguir en los próximos años.

1.4 Planificación del Trabajo

La planificación del trabajo se ha realizado acorde a las 11 semanas que se disponen según la planificación del aula del máster. En función de esto he generado una serie de objetivos a cumplir y estimado el tiempo necesario para realizarlos partiendo de la base de que la suma total debían ser 11 semanas. El resultado es el que se muestra en la gráfica siguiente.

	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana 10	Semana 11
Planificación											
Recolección de información											
Lectura											
Modificación del plan											
Redacción primeros puntos											
Primer feedback											
Modificación del plan											
Correcciones											
Redacción resto del trabajo											
Segundo feedback											
Últimas correcciones											
Entrega											

Planificación: Durante esta fase se establecerá el tema final y objetivos de trabajo, así como una primera idea de los capítulos a tratar.

Recolección de información: En base al tema y los objetivos se buscarán los libros y documentos necesarios para alcanzarlos.

Lectura: del material encontrado, así como de otros documentos que puedan surgir de la lectura de estos. De esta lectura se obtendrán notas y resúmenes.

Modificación del plan: En base a lo leído se ajustarán los capítulos a desarrollar en el trabajo de ser necesario.

Redacción primeros puntos: En base al nuevo ajuste y con lo leído se procederá a redactar los primeros puntos del trabajo.

Primer feedback: Se enviará al tutor esta primera redacción para su evaluación y comentarios.

Modificación del plan: En base a los comentarios del tutor se modificará el plan establecido de ser necesario.

Correcciones: En base a los comentarios del tutor se modificarán aplicarán los cambios y correcciones sugeridos en la redacción.

Redacción resto del trabajo: Se procederá a redactar el resto del trabajo tras las modificaciones ya comentadas.

Segundo feedback: Se enviará al tutor un borrador de la versión final para su evaluación y comentarios.

Últimas correcciones: En base a los comentarios del tutor se modificarán aplicarán los cambios y correcciones sugeridos en la redacción, disponiendo así ya de una versión final.

Entrega: Preparación y envío de la versión final para su evaluación.

1.5 Breve sumario de productos obtenidos

Como breve resumen se puede decir que en el presente trabajo se ha obtenido:

- Un breve resumen del contexto histórico reciente en materia de seguridad y privacidad.
- Un análisis de lo que el avance de la tecnología ha supuesto para la privacidad.
- Estudio de la legislación española en materia de videovigilancia.

- Análisis y comparación de diferentes posturas a la hora de tratar el uso de la videovigilancia con reconocimiento facial.

1.6 Breve descripción de los otros capítulos de la memoria

Ha continuación se hace un breve resumen del resto de los capítulos de este trabajo de fin de máster:

2.1 Presentación de la legislación española y las leyes tratadas: En esta capitulo se introduce la jerarquía por la que se rigen la normativa española y se listan las leyes más usadas durante este trabajo.

2.2 La excusa de la seguridad: Pequeño análisis histórico de la evolución del conflicto entre seguridad y privacidad desde los atentados del 11S.

2.3 La tecnología y la creciente recolección de datos personales: Análisis de lo que el avance de la tecnología ha supuesto para la privacidad.

2.4 La videovigilancia en España: Estudio de la legislación española en materia de videovigilancia.

2.4.1 Regulación de la videovigilancia de las fuerzas y cuerpos de seguridad del estado: Análisis de la legislación española que regula el uso de la videovigilancia por parte de los cuerpos y fuerzas de seguridad del estado.

2.4.2 La videovigilancia durante la instrucción de un caso: Análisis de la legislación española que regula el uso de la videovigilancia por parte de los cuerpos y fuerzas de seguridad del estado en la fase de instrucción de un caso.

2.4.3 RGPD y videovigilancia en España: Análisis de la RGPD en lo relativo a la videovigilancia.

2.4.4 LOPDGDD y videovigilancia: Resumen de los aspectos novedosos que aporta esta ley a lo ya visto hasta ahora en lo referente a videovigilancia.

2.5 La videovigilancia y el reconocimiento facial: Estudio de lo que supone la combinación de la videovigilancia con técnicas de reconocimiento facial prácticamente instantáneas.

2.5.1 El caso chino: Análisis del uso de la videovigilancia con reconocimiento facial en China.

2.5.2 El caso de San Francisco: Análisis del uso de la videovigilancia con reconocimiento facial en la ciudad de San Francisco.

2.5.3 España, RGPD y reconocimiento facial: Análisis del uso de la videovigilancia con reconocimiento facial en España.

2. Resto de capítulos

2.1 Presentación de la legislación española y las leyes tratadas.

A modo de inicio de este trabajo de fin de máster, creo que es conveniente citar los distintos tipos de normativas que pueden ser aplicables en materia de protección de datos en España, así como la jerarquía que las rige y que ayudará a comprender que norma prevalece sobre el resto en caso de conflicto.

Constitución española

Unión europea: directivas y reglamentos

Ley

Real Decreto

Si bien se han presentado las distintas normas en orden de mayor a menor, a continuación, se muestra un esquema que muestra el orden de prelación de estas.

Si bien la base de todo este trabajo gira entorno a la RGPD, existen otras normas que se evaluarán durante el presente trabajo al ser de aplicación directa al objeto del mismo. De esta forma, a continuación, se relata la legislación más importante a la cual se referenciará a lo largo del trabajo.

- Constitución española [2]

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD) [1]
- Ley Orgánica 4/1997, de 4 de agosto [3]
- Real Decreto 596/1999, de 16 de abril [4]
- Ley 5/2014, de 4 de abril, de Seguridad Privada [5]
- Ley Orgánica 15/1999 [6]
- Ley de Enjuiciamiento Criminal [7]
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) [8]

2.2 La excusa de la seguridad

Desde los atentados del 11 de septiembre de 2001, el mundo ha experimentado un cambio radical en todo lo referente al miedo a los ataques terroristas y especialmente a los ataques islamistas. Estos atentados junto con los que se produjeron más tarde en lugares como Madrid o Londres provocaron un miedo en toda la sociedad occidental, que vio amenazada su hasta entonces pacifica vida.

Si bien este miedo es hasta cierto punto justificado puesto que puso de manifiesto los fallos de los estados a la hora de gestionar amenazas, así como lo aparentemente sencillo que puede ser sembrar el terror en ciudades que cualquiera tildaría de tranquilas y seguras, la reacción de los estados a este miedo ha sido y es en muchas ocasiones desproporcionado.

Así pues, desde estos atentados, los estados han aprovechado y fomentado este miedo para desde justificar guerras hasta aumentar el control sobre su propia ciudadanía. Un buen ejemplo, es el ultimátum que George W. Bush dio a Sadam Husein antes del inicio de la guerra de Irak

> *“El régimen tiene una historia de agresiones en Oriente Medio. Odia profundamente a América y sus amigos, y ha ayudado, entrenado y dado cobijo a terroristas, incluidos miembros de Al Qaeda.” [9]*

Como se puede apreciar, Bush justifica el inicio de la guerra como una medida para garantizar la seguridad de EEUU y perseguir y castigar a los aliados de Al Qaeda. Precisamente, Bush ya adelantó en el discurso que dio el mismo 11 de septiembre que perseguiría tanto a los responsables como a los que les diesen asilo.

> *“Está en marcha la búsqueda de los que están atrás de estos actos malvados. He asignado la totalidad de los recursos de nuestras comunidades de inteligencia y ejecución de la ley a encontrar a los responsables y llevarlos ante la justicia. No distinguiremos entre los terroristas que cometen estos actos y aquellos que los acogen.” [10]*

Así mismo, este nuevo miedo creado por los atentados y potenciado tanto por las propias organizaciones terroristas como por los estados. Se usó, como ya se ha dicho, para aumentar las medidas de seguridad y control dentro de los propios estados, lo cual implica que los estados pasaron a vigilar de una forma mucho más activa a sus propios ciudadanos.

Quizás el mayor escándalo que ha ayudado a poner en primera línea el claro descontrol que ha existido durante los años posteriores al 11S sea el de Edward Snowden y el ya famoso programa PRISM.

Tal y como reveló Snowden a través de la publicación de varios documentos secretos, PRISM es un programa creado por la NSA para la recolección masiva de comunicaciones procedentes de las grandes compañías tecnológicas estadounidenses (Yahoo!, Microsoft, Apple etc.). Este programa fue puesto en marcha durante el año 2007 por George W. Bush gracias a la aprobación del llamado Protect America Act, conocido popularmente como US Patriot Act [11][12]. Y a la connivencia de la Foreign Intelligence Surveillance Court que debía supervisarlo, y que aprobó ordenes presentadas por el gobierno modificando el criterio que hasta entonces mantenían por el cual era necesario que el gobierno demostrase que el objetivo tenía una conexión clara con el terrorismo o el espionaje. Así pues, y gracias a este cambio de criterio, PRISM empezó a operar con la única garantía por parte del tribunal de que se comprobaría que se disponía de procedimientos razonables para la minimizar la recolección de datos de ciudadanos americanos sin una orden [13].

Así pues, gracias a los documentos filtrados por Snowden, la ciudadanía empezó a tomar conciencia de hasta donde habían llegado sus propios gobiernos bajo la excusa de la protección frente al terrorismo.

Gracias a todos estos casos revelados por los documentos filtrados por Snowden y otros “traidores” estadounidenses, en Europa hemos podido llegar a conocer ya no solo que nuestros datos y comunicaciones que pasaban por Estados Unidos eran espiados por el gobierno, sino que las propias agencias de inteligencia europeas colaboraban con sus homólogos estadounidenses y estos les daban acceso a los datos recabados mediante PRISM y otros programas. Así, por ejemplo, se ha descubierto que la agencia de espionaje británica obtenía datos de PRISM gracias a su colaboración con la CIA y NSA [13].

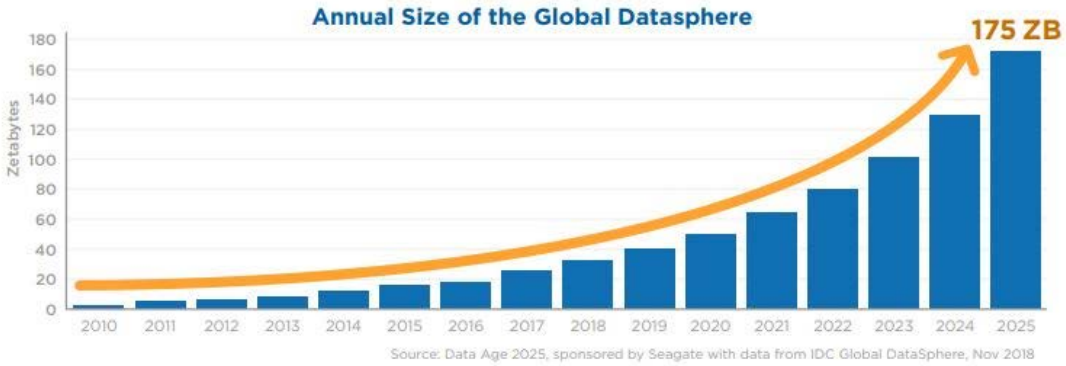
Cabe insistir en que, si bien esta recolección y análisis de datos masivos realizados por las agencias estadounidenses es alarmante, era en principio legal debido a la cobertura otorgada por todas las leyes aprobadas por Bush tras el 11S y siempre contaba con la autorización expresa del Tribunal de Vigilancia de Inteligencia Extranjera.

Como hemos visto, a raíz de los atentados del 11S y del creciente miedo que se propagó desde entonces alentado tanto por los propios terroristas a través de amenazas y nuevos atentados (Londres, Paris, Madrid, Barcelona etc.), como por gobiernos, estos últimos usaron este miedo

para, con el visto bueno de la opinión pública, aprobar leyes que restringían de forma clara la libertad y privacidad de los propios ciudadanos y abrían puertas a prácticas que cuanto menos eran cuestionables en asuntos de protección de datos. Pero toda esta maquinaria hecha para revelar los más mínimos secretos de aquellos considerados sospechosos casi de forma arbitraria algunas veces, no se sustentaba solo en lo que se obtenía de internet, sino que se alimentaba de otras fuentes como datos de pasajeros, cámaras de vigilancia etc. En resumen, esta gran maquinaria se ha vuelto lo que es hoy en día gracias al imparable avance de la tecnología.

2.3 La tecnología y la creciente recolección de datos personales

Desde el inicio de la era de la información, que tiene su comienzo en lo que ha venido a llamarse revolución digital o Tercera revolución industrial, la cantidad de información generada por el ser humano ha crecido de una forma sin precedentes y cada vez a mayor ritmo.



1 Crecimiento anual de la información [14]

Toda esta información que se genera día a día ha despertado la curiosidad de gobiernos y empresas, que han visto una oportunidad perfecta de recolectar información y tratarla para diferentes usos sin que en muchas ocasiones los propios usuarios de las tecnologías sean plenamente conscientes de los datos que dejan y el uso que se hace de los mismos.

2 Usuarios de la tecnología [15]

Según el último informe de *we are socia*l [15] en el que se hace un análisis del uso de internet, se rebela como internet tiene ya una penetración del 57% de la población mundial con un total de 4.388 billones de usuarios de los cuales 3.484 billones son usuarios de activos de alguna o varias redes sociales. Este volumen de usuarios, que crece día a día, genera un volumen de datos que las diferentes empresas y estados recogen y tratan casi siempre previa aceptación del usuario. Ahora bien, si nos paramos a pensar en esa aceptación de los usuarios al tratamiento de sus datos, nos daremos cuenta de ciertos problemas e incongruencias que surgen y que han llevado y llevan al abuso por parte de los recolectores.

Pero el avance y la expansión en internet por sí solas no suponen a priori un problema para la privacidad de las personas. Para que se produzca este riesgo del que ya se ha hablado, ha sido necesario que se junten la evolución tecnológica que ha permitido el tratamiento masivo de datos, así como la aparición de diferentes herramientas y servicios que recolectan datos de los usuarios. Todo esto en conjunto con la búsqueda de fuentes de ingresos de las empresas más la ambición de los estados de controlar a su propia ciudadanía, han creado toda una maquinaria, de la que aun, a día de hoy, somos a penas conscientes, en la que aparecen nuevas tecnologías y servicios cada día que nos hacen ceder cada vez más datos personales, haciéndonos así renunciar cada vez más a nuestra propia privacidad.

Así, por ejemplo, las compañías que surgen en el ecosistema de internet encuentran un filón en la recolección tratamiento y venta de datos de sus usuarios. De esta forma desde las cookies hasta los datos que damos al crear una cuenta en una web cualquiera, se han convertido en formas de generar ingresos para las compañías y en una de las mejores fuentes de datos de sus propios ciudadanos para los estados.

Todos estamos ya acostumbrados al típico aviso de la aceptación del uso de cookies si pretendemos seguir navegando por una determinada página web, o la típica checkbox que debemos marcar para darnos por enterados de las políticas de privacidad de una web o servicio en el cual estamos creando un usuario o dándonos de alta. Todos estos métodos al final son solo la cobertura legal que necesitan las empresas para defender el tratamiento y la recolección de datos que llevan a cabo. De hecho, hasta la entrada en vigor de la RGPD, las empresas tenían bastante más libertad a la hora de explicar que datos y que uso se hacían de los mismos. Y aunque si bien esta nueva regulación ha mejorado desde el punto de vista de la privacidad, la información disponible y los límites que las empresas deben cumplir a la hora de recolectar y usar estos datos todavía sigue quedando mucho en lo que avanzar.

Un buen ejemplo es el de las checkbox y cookies que comentábamos. Según Paloma Llaneza en su libro Datanomics [16] si bien los usuarios son ahora más conscientes y se preocupan más por qué datos ceden y qué se hace con ellos, casi nadie se lee las políticas de privacidad ni los

avisos de las cookies. Este hecho, no se produce tanto por vaguería sino por el increíble tiempo que le llevaría un usuario leerse todos los avisos de las webs que consulta y que se estima en 25 días al año según un estudio de 2008 [17]. Por lo que podemos sacar la conclusión de que por mucho que se obligue a las empresas a aclarar qué uso se hace de los datos que recolectan, nadie o casi nadie lo leerá y todos terminaremos aceptando el tratamiento con tal de acceder al servicio.

Esta cesión de cada vez más datos personales de forma medio consciente no se ha producido de la noche a la mañana, sino que ha sido un proceso paulatino. Por poner un ejemplo Google, al principio solo disponía de datos de navegación y búsquedas procedentes de sus cookies y sus datos de búsquedas, pero con el paso del tiempo se han añadido los datos de tu cuenta de mail, todo lo relacionado con YouTube, con los datos de su servicio de anuncios para páginas webs, sin olvidarnos de los datos obtenidos de los móviles gracias a Android entre los que en muchas ocasiones se encuentra no solo la geolocalización sino grabaciones de audio gracias a su asistente de voz. Todos estos datos que Google puede cruzar entre ellos pueden resultar ya no solo en la obtención del perfil de una persona, sino también en la obtención de rutinas, rutas habituales, lugares que visitas a menudo que si se cruzan con las horas y días pueden darle a Google información sobre dónde y de que trabajas y así un largo etcétera. En resumen, una empresa privada que se ha expandido lo suficiente es capaz de conocer y predecir ya no solo tus gustos y aficiones, sino que también puede predecir con bastante exactitud donde estarás un día a una hora determinada.

Todo esto ya es de por sí bastante preocupante, pero al igual que empresas como Google no ha llegado a este punto de forma progresiva, es muy probable que en el futuro sean capaces de llegar aún más lejos. Una buena idea de hasta qué punto podían llegar estas empresas y los estados está en el concepto de Smart City.

La Smart City es un concepto que a raíz de la irrupción del 5G y de la realidad que ya supone el internet de las cosas (IoT) se ha hecho bastante popular. El concepto podría resumirse como una ciudad en la que todos sus elementos están conectados, desde farolas y semáforos inteligentes que se autorregulan solos y se comunican con los vehículos y peatones de forma automática, hasta coches que se comunican entre ellos y se conducen solos y autogestionan el tráfico de la ciudad. Al final se trata de una especie de conciencia colmena que permite a una ciudad funcionar de forma más eficiente.

Esta utopía que venden las empresas y gobiernos en un ejercicio de paternalismo positivo oculta un gran riesgo para la privacidad. Este riesgo consiste en que en una ciudad donde todo está conectado, toda acción que realizas se monitoriza, graba y genera una respuesta para adaptar la ciudad a tus necesidades, es decir, nada de lo que hagas será privado, siempre habrá mínimo un rastro en internet al que alguien malintencionado podría acceder para obtener un beneficio. Y no solo eso,

sino que las empresas y gobiernos que ponen a disposición estas tecnologías querrán obtener un beneficio de todos estos nuevos datos.

En resumen, desde que entramos en la llamada era de la información, el avance exponencial de la tecnología ha facilitado y dado nuevas oportunidades a los seres humanos, pero este avance continuo tiene un lado negativo. Este lado negativo consiste en que empresas y estados han utilizado todas estas tecnologías en su propio beneficio, haciendo un especial foco en la expansión de tecnologías de control y recolección de datos que van desde cámaras de seguridad, pasando por cookies hasta historiales de GPS, con el único objetivo de conocer, predecir y vigilar a sus propios ciudadanos o usuarios.

Ante todos estos nuevos métodos de recolección y tratamiento de la información, las leyes existentes se han mostrado claramente obsoletas, e incluso se ha descubierto que los estados en algunos casos habían modificado estas leyes para legalizar estos nuevos usos. Pero gracias a determinadas noticias y escándalos como los vistos anteriormente, los legisladores están empezando a reaccionar ante la demostrada amenaza contra la privacidad que suponen ciertas prácticas que aun hoy en día están normalizadas, y están modificando las leyes para intentar adaptarlas a los nuevos tiempos.

A este respecto, merece especial atención el caso concreto de la videovigilancia ya que es uno de los que supone un mayor riesgo para la privacidad, y además es uno de los recursos que mayor expansión ha tenido.

2.4 La videovigilancia en España

Como se ha visto en el punto anterior, el avance y consecuente abaratamiento de la tecnología han permitido a empresas y estados obtener de forma más o menos sencilla datos de todo tipo de sus propios ciudadanos. Pero quizás uno de los cambios que hasta ahora ha podido pasar más desapercibido puesto que ya desde hace años los ciudadanos estamos acostumbrados a este tipo de vigilancia y porque ya casi forma parte del paisaje urbano de los centros de muchas ciudades, es el de la cámara de videovigilancia.

Al igual que en la mayoría de la tecnología con una cierta antigüedad, las cámaras de videovigilancia han sufrido un gran crecimiento en la última década gracias a internet y el famoso internet de las cosas. Y al igual que en otros muchos casos este avance que ha llenado el mercado de multitud de modelos y soluciones de videovigilancia basadas en cámaras IP, han traído multitud de problemas, siendo quizás el mayor de ellos lo sencillo que resulta hackearlas y acceder a su contenido [18].

Se podría caer en la tentación de pensar que estos fallos en la seguridad son solo cosa de las cámaras que se venden al público en general y que

las cámaras que usan las fuerzas armadas y la policía usan otras tecnologías y son mucho más seguras, pero la realidad es que nada escapa de estas vulnerabilidades y otras más o menos graves que se han llegado a detectar en los dones usados por el ejército estadounidense [19].

Adicionalmente, el hecho de que las cámaras sean cada vez más baratas y su uso se esté simplificando mucho hasta el extremo de que ya muchas apenas si hay que simplemente enchufarlas y conectarlas a internet, ha provocado que cada vez más se están convirtiendo en un complemento para facilitar las labores de vigilancia de las fuerzas y cuerpos de seguridad, así como de la seguridad privada. Como se decía anteriormente, es ya normal encontrar en aeropuertos, calles céntricas, centros comerciales o casi cualquier edificio con actividad pública o abiertos al público multitud de cámaras de videovigilancia. Pero también es cada vez más común que la propia policía haga uso de cámaras móviles para el control de manifestaciones y grandes eventos.

Por todos estos motivos y también por los de las nuevas capacidades que surgen con el avance de la tecnología la agencia española de protección de datos publicó la “Guía sobre el uso de videocámaras para seguridad y otras finalidades” [20] así como una sección en su web a este respecto [21], que aclara todas las dudas respecto a la legislación aplicable, así como algunas de los casos en los que hay dudas respecto a la RGPD y la videovigilancia.

En España, la video vigilancia está regulada por varias leyes y reglamentos, cada uno de los cuales se creó para regular los distintos ámbitos de aplicabilidad de la video vigilancia. A continuación, se listan las leyes españolas a este respecto y el ámbito que pretenden regular dentro de la videovigilancia:

- Ley Orgánica 4/1997, de 4 de agosto que regula la videovigilancia para los cuerpos y fuerzas de seguridad del estado. [3]
- Real Decreto 596/1999, de 16 de abril, que aprueba el reglamento de desarrollo y ejecución de la anterior ley. [22]
- Ley 19/2007, de 11 de julio, en la que se regula el uso de la videovigilancia en eventos deportivos. [23]
- Real Decreto 203/2010, de 26 de febrero, que aprueba el reglamento de desarrollo y ejecución de la anterior ley. [24]
- Ley 5/2014, de 4 de abril, de Seguridad Privada. [5]
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) [8]

2.4.1 Regulación de la videovigilancia de las fuerzas y cuerpos de seguridad del estado

Como se ha visto la videovigilancia en España, está regulada por la Ley Orgánica 4/1997, de 4 de agosto [3] y su reglamento de desarrollo aprobado en el Real Decreto 596/1999, de 16 de abril [22].

Una de las primeras cosas que fija esta ley que regula la videovigilancia de los cuerpos de seguridad del estado, es el procedimiento y las garantías que deben existir a la hora de aprobar la instalación uso de cámaras fijas y móviles. Esta diferenciación entre fijas y móviles resulta bastante importante, puesto que las móviles entrañan más riesgos a la hora de controlar qué se graba y así garantizar que no se atenta contra las libertades fundamentales de los ciudadanos. Es por esta razón que se establece una diferencia en los procedimientos a la hora de autorizar su uso.

Respecto de las cámaras fijas, la autorización tal y como establece el artículo tres de la Ley Orgánica 4/1997, de 4 de agosto [3] debe ser aprobada por el delegado del gobierno de la comunidad, tras haberse emitido un informe por una comisión de garantías que debe estar presidida por el presidente del Tribunal Superior de Justicia de la misma Comunidad, siendo el resto de la composición detallado en el Real Decreto 596/1999, de 16 de abril [22].

> *"2. Las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales serán autorizadas por el Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la misma Comunidad. La composición y funcionamiento de la Comisión, así como la participación de los municipios en ella, se determinarán reglamentariamente." [3]*

Así mismo, tal y como establecen los artículos 3.3 y 4, para autorizar su uso se deben tener en cuenta de acuerdo con el principio de proporcionalidad los criterios:

- Asegurar la protección de los edificios e instalaciones públicas y de sus accesos.
- Salvaguardar las instalaciones útiles para la defensa nacional
- Constatar infracciones a la seguridad ciudadana
- Prevenir la causación de daños a las personas y bienes.

De esta forma, si el informe emitido por el comité considerase que se vulnera alguno de los criterios mencionados, no se podrá proceder a la instalación de las cámaras.

> *"3. No podrá autorizarse la instalación fija de videocámaras cuando el informe de la Comisión prevista en el apartado segundo de este artículo estime que dicha instalación supondría una vulneración de los criterios establecidos en el artículo 4 de la presente Ley Orgánica." [3]*

> ***"Artículo 4.*** *Criterios de autorización de instalaciones fijas.*
>
> *Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes." [3]*

Respecto de las cámaras móviles, se especifican dos usos diferentes en el artículo 5. El primero es su uso como complemento en zonas donde existen cámaras fijas, pero siempre debe ser su uso justificado por peligro concreto.

> *"1. En las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, podrán utilizarse simultáneamente otras de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6." [3]*

El segundo supuesto, consiste en el uso de cámaras móviles en el resto de lugares públicos. Para este supuesto, la autorización la realizará el máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad. No obstante, será necesario emitir un informe de autorización que será remitido en un máximo de 72 al comité anteriormente mencionado para su evaluación. Adicionalmente, se prevé el caso de tener que realizar grabaciones sin disponer del tiempo de obtener la autorización, en cuyo caso se dispondrán de 72 horas para realizar un informe en el que se expliquen las causas que han llevado a tal situación y que debe remitirse al el Máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la comisión para su evaluación. Si la evaluación saliese negativa por cualquier motivo la ley prevé que las grabaciones deben ser destruidas de forma inmediata.

> *"2. También podrán utilizarse en los restantes lugares públicos videocámaras móviles. La autorización de dicho uso corresponderá al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización del medio a los principios previstos en el artículo 6.*
> *La resolución motivada que se dicte autorizando el uso de videocámaras móviles se pondrá en conocimiento de la Comisión prevista en el artículo 3 en el plazo máximo de setenta y dos horas, la cual podrá recabar el soporte físico de la grabación a efectos de emitir el correspondiente informe.*

En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, se podrán obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión aludida en el párrafo anterior, la cual, si lo estima oportuno, podrá requerir la entrega del soporte físico original y emitir el correspondiente informe.
En el supuesto de que los informes de la Comisión previstos en los dos párrafos anteriores fueran negativos, la autoridad encargada de la custodia de la grabación procederá a su destrucción inmediata." [3]

Como se ha visto, la ley en un principio sienta las bases de los supuestos en los que se puede solicitar la videovigilancia, así como en los procedimientos e instituciones que deben autorizar y garantizar su buen uso.

Una vez cubiertos estos aspectos, la ley pasa a una zona donde se pretende garantizar el buen uso de estas grabaciones especificando sus principios de uso, tiempo de conservación de las grabaciones y otros aspectos que garanticen la privacidad y correcta protección de los datos de carácter personal que estas cámaras dada su función recogen.

Así pues, el artículo 6 especifica los principios de utilización de las video cámaras. Este, desde el punto de vista de la privacidad y la protección de datos resulta un artículo fundamental, puesto que entre otras cosas recoge que el uso de las videocámaras debe regirse por el principio de proporcionalidad, entendido como idoneidad e intervención mínima. Es decir, que en principio solo debería aprobarse el uso de la videovigilancia en una versión mínima y siempre y cuando sea estrictamente necesario, evitando así la proliferación masiva de cámaras. Este aspecto, dado el espectacular crecimiento que se aprecia a simple vista en cualquier centro urbano, podría decirse que en muchos casos se está aplicando de forma no muy estricta, pero si es cierto que fuera de los centros de las ciudades esta videovigilancia se relaja y por lo tanto se podría llegar a entender y justificar como la protección extra de lugares de amplio transito ya que son lugares de alto riesgo al ser objetivo de ataques y altercados, y que es precisamente el supuesto que exige el artículo 6.4

"1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.

2. La idoneidad determina 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 esta Ley.

3. La intervención mínima exige la ponderación, 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.
4. La utilización de videocámaras 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." [3]

El último punto del artículo 6 quizás sea uno de los más interesantes desde el punto de vista de la privacidad, puesto que prohíbe expresamente las grabaciones de imagen y sonido del interior de viviendas y vestíbulos, así como de conversaciones privadas sin la debida autorización judicial. Además, obliga a la eliminación de cualquier imagen y sonido obtenido accidentalmente en cualquiera de los casos mencionados.

"5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza
estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia." [3]

Finalmente, uno de los artículos finales que tiene una importancia determinante sobre la privacidad y protección de datos, es el artículo 8 que fija el plazo máximo de conservación de las grabaciones en un mes, excepto en los casos en los que las grabaciones estén relacionadas con hechos penales. Adicionalmente, se prohíbe la cesión de estas a terceros y se obliga a las personas con acceso a ellas a respetar la confidencialidad sobre las mismas.

"1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las
mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.

3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo." [3]

Con esto queda cubierto el caso de la vigilancia con fines de vigilancia preventiva, es decir, vigilancia en la que no se está investigando un delito en concreto si no que se trata de investigar una amenaza o prevenir posibles delitos. Ahora bien, en España también está regulado el supuesto de la videovigilancia durante la instrucción de una causa.

2.4.2 La videovigilancia durante la instrucción de un caso

Como ya se ha dicho, el uso de la video vigilancia durante la fase de instrucción de un caso también se encuentra regulado de forma específica dentro de la legislación española. En concreto, se recoge en los capítulos IV y VII del título VIII de la Ley de Enjuiciamiento Criminal [7].

El título de este artículo "*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*" hace una referencia expresa al artículo 18 de la constitución que es el que consagra el derecho al honor, la intimidad y la imagen.

> *"Artículo 18*
>
> 1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> 2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
>
> 3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
>
> 4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos." [2]*

Como se puede observar, la constitución hace especial énfasis en la limitación que debe hacerse de la informática para preservar estos derechos fundamentales. De esta forma, el título VIII de la Ley de Enjuiciamiento Criminal especifica los supuestos y la forma en los que se pueden limitar estos derechos fundamentales, y más específicamente en sus capítulos IV y VII se recogen los casos y la manera de proceder cuando las fuerzas de seguridad pretenden realizar grabaciones de un investigado.

Dentro del capítulo IV ya mencionado es especialmente interesante el artículo 588 bis a que recoge los principios rectores que deben cumplirse para poder proceder a la videovigilancia de un investigado.

> "*Artículo 588 bis a. Principios rectores.*

1. *Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.*
2. *El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.*
3. *El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.*
4. *En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:*
    a) *cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o*
    b) *cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.*
5. *Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho." [7]*

Así pues, en estos casos al igual que como ya hemos visto anteriormente, la previa autorización de un juez es un requisito indispensable sin la cual no se puede realizar ninguna grabación. También deben darse una serie de condiciones ya vistas como son la idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida que garantizarán que la medida es la única posible y que daña lo menos posible los derechos del investigado. Adicionalmente, el artículo introduce el principio de especialidad, por el cual solo se podrá realizar la videovigilancia de un investigado para un delito concreto y nunca con el finde prevenir o descubrir uno.

Respecto del resto de artículos del capítulo IV, comentan las formas y contenido de las solicitudes que deben hacer los cuerpos de seguridad del estado al juez para solicitar el inicio de la vigilancia, así como los plazos que deben seguirse incluyendo el de destrucción del material obtenido que se sitúa por lo general en 5 años.

> *"Artículo 588 bis k. Destrucción de registros.*
>
> 1. *Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial.*
> 2. *Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.*
> 3. *Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados." [7]*

En cuanto al capítulo VII es de especial interés su primer artículo ya que regula la grabación de imágenes de un investigado en lugares públicos en los que como es inevitable pueden salir terceras personas.

> *"Artículo 588 quinquies a. Captación de imágenes en lugares o espacios públicos.*
>
> 1. *La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.*
> 2. *La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación." [7]*

Como se puede ver la grabación de un investigado en un lugar público estará autorizada siempre y cuando sea necesaria para la investigación. Respecto a la aparición de terceras personas, el artículo deja claro que de existir una conexión entre el tercero y el investigado o entre el tercero y los hechos investigados, la grabación puede realizarse; y en el caso de

que el tercero no tenga relación ni con los hechos ni con el investigado, podrá realizarse siempre y cuando el hecho de pararla afectase gravemente la utilidad de la vigilancia.

Con esto quedaría cubierto el supuesto de la videovigilancia en caso de una investigación judicial. Como se ha visto, este caso no dista mucho de la videovigilancia para vigilar y prevenir vista con anterioridad ya que requiere de la previa autorización de un juez y siempre deben darse una serie de garantías antes de que el juez acepte la medida. Aun así, existe una diferencia fundamental para este caso, puesto que la medida de videovigilancia puede incluir el interior del hogar de una persona cosa que para el resto de casos, está terminantemente prohibida. Esta diferencia fundamental de la que hablo no es otra que el principio de especialidad que garantiza que este tipo de videovigilancia solo se puede aprobar para la investigación de delitos concretos y nunca para descubrir un delito. Este punto, si bien puede uno caer en la tentación de diluirlo entre el resto de principios necesarios, quizás sea el más importante puesto que es el que nos protege de una vigilancia al más puro estilo de la novela de George Orwell, 1984.

Una vez vistas estas leyes, cabe preguntarse, qué efectos ha tenido la RGPD sobre ellas. Es por esta razón que la Agencia española de protección de datos publico la guía ya mencionada con anterioridad, así como una serie respuestas a consultas de diversas empresas y administraciones referentes a este tema.

2.4.3 RGPD y videovigilancia en España

Si nos centramos únicamente en lo que respecta a las fuerzas y cuerpos de seguridad del estado, la RGPD ha tenido un impacto al igual que en cualquier empresa que trata datos de carácter personal, pero gracias a la garantía que ofrece el artículo 6.1 que garantiza el tratamiento de datos si se realiza por motivos de bien de interés público, este impacto se limita únicamente a cómo se gestionan las grabaciones, y no al derecho a realizarlas dejando por lo tanto la Ley Orgánica 4/1997, de 4 de agosto [3] intacta a este respecto.

> *"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
>
> *…*
>
> *e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;" [3]*

Ahora bien, tal y como se explica en varias notas publicadas por la agencia de protección de datos [25][26], la RGPD introduce una novedad al considerar que tanto las cámaras que graban como aquellas que simplemente captan, pero no almacenan ni el audio ni el video, realizan

un tratamiento de datos de carácter personal y por lo tanto deben ajustarse a la RGPD. Esta justificación de que se produce tratamiento parte de la base de que toda imagen de una persona en la que se le pueda identificar supone en virtud del artículo 4.2 [1] un tratamiento de datos personales, y por lo tanto todo lo establecido en la RGPD al respecto de cómo deben tratarse los datos, y los derechos de los usuarios incluido el de información deben ser respetados.

> *"A este respecto, debe partirse de que la imagen de una persona identificada o identificable constituye un dato personal, cuyo tratamiento está sujeto al RGPD, teniendo en cuenta que su artículo 4.2) define tratamiento como: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción." [25]*

Es decir, tal y como establece la agencia española de protección de datos, antes de la RGPD al no existir una grabación no tenían la obligación de inscribirse, pero ahora deben realizar el registro de actividades de tratamiento al considerarse como un tratamiento de datos personales.

> *"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."* [20]

Otro caso interesante que ha surgido en los últimos años y que es interesante analizar desde el punto de vista ya no solo de la RGPD sino de la propia ley de videovigilancia, es el de los drones.

En vista de lo contado hasta ahora, parece claro que al existir una cámara de por medio, ya se produzca o no una grabación, existirá un tratamiento de datos y por lo tanto se deberá aplicar lo establecido en la RGPD. Pero tal y como explica la agencia española de protección de datos en otra de sus respuestas a consultas [27], existe un componente añadido ya que las personas que están siendo grabadas seguramente no sepan que lo están siendo, y por lo tanto desconozcan el tratamiento que se está realizando de sus datos personales.

> *"Pero existe además un componente añadido que es que en muchos casos ni la misma existencia del dron ni el tratamiento de los datos realizados por el mismo será conocido por el interesado*

o afectado habida cuenta de las propias características del aparato, que pueden volar y recoger datos sin necesidad de ser visto por las personas y sin estar sujeto a concretas barreras físicas al desplazarse por el aire." [27]

Así pues, la obligación de informar a los afectados se ve complicada por las especiales características del dron. Para esto, la agencia española de protección de datos recomienda que se trate de informar mediante diferentes canales, e incluso se informe de las operaciones realizadas en la web del operador del dron.

"El grupo de trabajo del 29 recomienda una aproximación "multicanal" habida cuenta de las limitaciones que una aproximación tradicional a la información tiene. Además recomienda, como buena práctica adicional, que los operadores de drones publiquen en su página web información que permita conocer las diferentes operaciones que han realizado o las que se proponen realizar en el futuro cercano, así como la posibilidad de insertar anuncios en periódicos, folletos o posters, o incluso mediante buzoneo." [27]

No obstante, la propia RGPD en su artículo 14.5 [1] establece que, si la comunicación resultase un esfuerzo desproporcionado, es posible no realizarla. Esto por lo tanto deja en manos del responsable determinar si el esfuerzo de informar a los afectados es o no desproporcionado. No obstante, de serlo se deberá garantizar que se adoptan las medidas oportunas que garanticen los derechos, libertades e intereses legítimos de los afectados.

"El art. 14.5 del RGPD establece que no se cumplirá con este derecho de información "cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información".

Pues bien, habida cuenta de que en todo caso se requiere el derecho de información en la recogida de datos a los interesados, corresponde al responsable valorar si se trataría de un esfuerzo desproporcionad cumplir con este derecho, y en todo caso, de ser así, tendría que adoptar las correspondientes medidas como indica el artículo anteriormente transcrito, incluso haciendo pública la

información.” [27]

Finalmente, cabe recordar que la instalación de cámaras en lugares públicos para labores de videovigilancia está reservada única y exclusivamente a las fuerzas y cuerpos de seguridad del estado, y que por lo tanto cualquier uso particular de videovigilancia con drones deberá ser realizado en lugares privados. Así mismo, los drones se consideran como es lógico a todos sus efectos cámaras móviles, por lo que regirán los principios para su uso y aprobación establecidos en la Ley Orgánica 4/1997, de 4 de agosto [3].

Antes de cerrar este capítulo del uso de drones, merece la pena detenerse en dos aspectos de la RGPD que deben ser considerados al usar drones con cámaras y en especial al ser usados para labores de videovigilancia.

El primero de ellos es el de la proporcionalidad, esta medida no solo está contemplada en la RGPD, sino que también aparece en todas las leyes vistas hasta ahora y que regulan el uso de cámaras independientemente del motivo. Así pues, deberá estar presente desde la toma de decisión de usar o no un dron con cámara, sino que también deberá tenerse en cuenta a la hora de analizar el uso o tratamiento que se pretende realizar de las imágenes tomadas con el dron.

El segundo es el principio de responsabilidad proactiva. Este principio es uno de los pilares en los que se basa la RGPD, ya que implica que el responsable del tratamiento lo es también de garantizar y demostrar que el tratamiento de los datos es conforme a la ley.

“Artículo 5
Principios relativos al tratamiento

…

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).” [1]

De hecho, la propia Agencia Española de Protección de Datos ha creado un apartado específico para explicar este concepto y todo lo que implica según la RGPD, haciendo especial énfasis en las medidas que se deben tomar para poder cumplir con dicho principio [28].

Con esto quedan cubiertos los efectos de la RGPD sobre la videovigilancia, pero la propia UE deja cierto margen de maniobrabilidad a los estados a la hora de adaptar su legislación para que cumpla con la RGPD. En el caso de España esta adaptación cobró forma con la

publicación de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) [8].

2.4.4 LOPDGDD y videovigilancia.

La LOPDGDD, aunque en lo sustancial no introduce grandes cambios respecto a la RGPD, sí que hace una mención especial a la videovigilancia en su artículo 22.

> *"Artículo 22. Tratamientos con fines de videovigilancia.*
>
> *1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.*
>
> *2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.*
>
> *No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado..." [8]*

Como se puede apreciar, aun siendo una mención específica, simplemente viene a reafirmar lo ya visto hasta ahora tanto en la RGPD como en el resto de las leyes, y que no es otra cosa que la vía pública solo se debe grabar cuando sea imprescindible, lo cual en la practica deja a las fuerzas y cuerpos de seguridad como la única autoridad que puede videovigilarla, con la ya sabida excepción de los bienes e instalaciones estratégicos etc.

> *"3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación." [8]*

Por otro lado, como se puede ver, también se hace mención a la duración específica de cuanto tiempo se pueden almacenar las imágenes y sonidos grabados, que se fija en un mes.

> *"4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente*

visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.
En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento" [8]

Este punto, resulta de interés puesto que uno de los pilares fundamentales de la RGPD es el derecho a la información de los afectados, y si bien, el punto especifica que para cumplir con el derecho de información basta con incluir un cartel que informe de la existencia de un tratamiento, de quién es el responsable y de que se pueden ejecutar los derechos previstos en la RGPD, los legisladores también se han visto forzados, a incluir una frase en la que se especifica que el responsable del tratamiento tendrá a disposición de los afectados toda la información a la que obliga la GDPR a este respecto.

Por último, el punto sexto del artículo merece una mención especial puesto que hace referencia explícita al caso de las fuerzas y cuerpos de seguridad del estado, estableciendo la regulación específica que deberán seguir dichos cuerpos.

"6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica." [8]

La directiva UE 2016/680 [29] a la que se refiere el punto, establece las directrices a seguir por los países miembros en lo referente al tratamiento de datos personales por parte de los cuerpos y fuerzas de seguridad del estado. Y aunque esta directiva parezca realmente interesante, un rápido análisis revela que conocida la RGPD y LOPDGDD, no se introduce grandes novedades. No obstante, sí que merece la pena comentar algunos aspectos y aclaraciones que introduce esta directiva respecto a lo ya visto.

Así por ejemplo en su artículo 8 en el que se habla de la licitud del tratamiento, simplemente se especifica que los cuerpos de seguridad del estado entenderán legitimado el tratamiento cuando actúen:

"… con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública…" [29]

Es decir, lo que en la RGPD se viene a llamar interés público.

Por otro lado, el artículo 15 si introduce un aspecto muy interesante como es las causas por las que un estado puede limitar el derecho de los afectados a ser informados, así como su derecho al acceso, y que se podrían resumir en que un estado puede limitar estos derechos cuando se estime que pueden poner en riesgo las razones del tratamiento y por lo tanto la seguridad pública.

"Artículo 15 Limitaciones al derecho de acceso

1. Los Estados miembros podrán adoptar medidas legislativas por las que se restrinja, total o parcialmente, el derecho de acceso del interesado siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas." [29]

Respecto al resto de artículos, no existen grandes novedades con respecto a la RGPD, limitándose de esta forma, a comentar temas ya tratados como la prevención de decisiones automatizadas, obligaciones del responsable del tratamiento etc.

Como se ha visto hasta ahora, la ley española en conjunto con la normativa europea de protección de datos, parecen ciertamente garantistas en lo referente al tratamiento de datos y la videovigilancia. Ahora bien, cabe preguntarse si al igual que pasó en EEUU con la administración Bush tras los atentados del 11S ya mencionado en la introducción, es posible hacer una reinterpretación de la normativa existente que autorice a los cueros de seguridad del estado a recolectar datos en casos que hasta ahora con el criterio actual se denegarían. Si pensamos en el caso de los drones, en principio al ser una cámara móvil

solo se podría usar ante un riesgo real y concreto. Este es el caso por ejemplo de manifestaciones y eventos que reúnen a multitudes de personas.

Pues bien, si esos eventos suponen un riesgo concreto de forma evidente, nada impide pensar que ante un nivel muy elevado de la alerta antiterrorista en la que se asume que existe un riesgo muy alto de amenaza, o ante alguna información recaba por los servicios de inteligencia basada en un rumor que alguien interprete como fiable, el comité de garantías y el máximo responsable autoricen el uso de drones para la vigilancia de posibles objetivos de un ataque, como el centro de las ciudades. Esta situación, en la que la amenaza se basa en hechos puramente subjetivos es por definición puramente interpretable y se podría autorizar una videovigilancia que más tarde podría muy bien demostrarse inútil si se descubre que la amenaza era ficticia o simplemente estaba sobredimensionada.

Todas estas situaciones en principio podrían pasar inadvertidas o minimizarse el impacto ante la ya manida excusa de la seguridad, y que entre tantas personas la vulneración ante la posible identificación de una se diluye al complicarse la identificación. No obstante, si se introduce una de las nuevas tecnologías que a día de hoy provoca mucha controversia en el campo de la videovigilancia, estos riesgos desaparecen y se crean nuevos, que hacen poner en tela de juicio el uso a la ligera de la videovigilancia. Esta tecnología a la que me refiero es el reconocimiento facial.

2.5 La videovigilancia y el reconocimiento facial.

Antes de comenzar este capítulo, merece la pena recordar lo visto al inicio de este trabajo en lo referente al contexto histórico que ha puesto de actualidad la privacidad, y cómo la tecnología permite recolectar y cruzar datos personales de forma masiva. Así pues, entre otras consideraciones es de especial interés volver a destacar cómo desde los atentados del 11S y gracias al implacable avance de la tecnología, empresas y estados han empezado a recabar cada vez más datos de sus clientes y ciudadanos respectivamente, unos con la excusa de ofrecer un mejor servicio e incluso gratuito y los estados mediante la excusa de la seguridad amparándose en el miedo a veces fomentado desde los mismos estados. Bajo este paradigma, se han invertido grandes cantidades de dinero y se han creado leyes, que han permitido durante años no solo recolectar estos datos sin dar explicaciones de por qué eran necesario y que se hacía con ellos, sino que han fomentado el intercambio de estos datos y su tratamiento con diversos fines entre los que se incluyen la vigilancia de los propios ciudadanos, y que no ha empezado a verse sometido a controles cada vez en apariencia más estrictos, hasta que la prensa no ha empezado a revelar los abusos cometidos en aras de nuestra seguridad o de la promesa de un servicio más personalizado. De esta forma, hemos

asistido al principio con indiferencia, pero cada vez con mayor estupor y preocupación, a como la frontera entre la privacidad y el legítimo derecho a la defensa y protección de los estados, se difumina cada vez más.

Como se ha comentado, todo esto no habría sido posible sin los continuos avances en la tecnología que cada vez mejoraban y ampliaban los datos recogidos y el tratamiento que se hacía con ello. Si bien, muchas de las tecnologías empleadas merecen una mención especial, para el tema de la videovigilancia que es tema central de este trabajo, es de especial interés la irrupción del reconocimiento facial.

Si bien el reconocimiento facial no es un método nuevo, puesto que de forma manual ya se usaba desde los años 60, al igual que en otros muchos casos la tecnología ha permitido mejorarlo tanto en precisión como en rapidez e incluso alcance. Los avances en tratamiento de imágenes, la mejora de la resolución de las cámaras, los métodos de Big Data, redes neuronales etc. pueden aplicarse todos a las imágenes recogidas por cámaras de videovigilancia y aplicar el reconocimiento facial de forma casi instantánea. De esta forma, podría no llegar a ser necesario el grabar las imágenes ya que la identificación se produce en el momento y puede actuarse. Afortunadamente como ya se ha visto, la RGPD hace explícitamente referencia al hecho de que no hace falta que las imágenes se graben para considerar que existe un tratamiento y es de aplicación el reglamento.

Ahora bien, cabría pensar que, si bien la tecnología existe y es aplicable, no es tan sencillo encontrar una base de datos que no pertenezca al estado con la que comparar las imágenes tomadas por la cámara. Pero la realidad, es que nuestras imágenes asociadas incluso a nuestro nombre, dirección y otros muchos datos personales ya están en bases de datos más o menos públicas y que han sido subidas e incluso cedidas por nosotros mismos. En concreto, un simple análisis de la mitad de las principales redes sociales como Facebook o Instagram te permiten obtener un nombre, una cara e incluso una dirección de millones de personas.

Como ya se ha mencionado más de una vez en este trabajo, internet y las nuevas tecnologías han ido metiendo en la cabeza de la gente que entregar sus datos personales de todo tipo a cambio de un servicio, una rebaja o cualquier otro motivo, no solo es lo normal y aceptable sino que redunda en tu beneficio ya que además obtendrás un servicio más personalizado, y lo que las empresas hagan con tus datos no importa puesto que quien no tiene nada que ocultar, no tiene nada que temer. Ahora bien, si esos datos que tan alegremente cedemos todos los días se empiezan a usar para otros fines y se cruzan con nuevos datos, quizás lleguemos a ver que nuestra privacidad está amenazada.

Un ejemplo curioso y que no costaría imaginar aplicado al reconocimiento facial, es de las empresas que secuencian tu ADN. Estas empresas han sido utilizadas por las autoridades como fuente de datos con la que

comparar los restos de ADN de los casos sin resolver, llevando en varias ocasiones a la detención de los culpables que, si bien no estaban en la base de datos directamente, fueron identificados gracias a un pariente que sí que lo estaba. [16]

Otro ejemplo ya directamente relacionado con la video vigilancia es el que podemos encontrar, al igual que el anterior, en el libro de Paloma Llaneza [16], en el que da a conocer un sistema capaz de identificar a una persona en el momento de bajar del avión y seguirla por todo el país hasta que lo abandona. Si bien este sistema ya es escalofriante de por sí ya que no se aclara bajo qué criterios funciona, la cosa empeora al conocer que el sistema además permite reconocer e identificar los objetos que el vigilado lleva y deja, así como analizar los gestos de la gente e identificar gestos y comportamientos sospechosos.

Trasladando todo esto a la videovigilancia, podemos llegar a la conclusión, de que tanto las cámaras en vía pública como en espacios públicos, pero de gestión privada como los centros comerciales, son susceptibles de poder incorporar un sistema de reconocimiento facial que con una gran probabilidad pueda identificarnos ya sea mediante una base de datos del gobierno (DNI) como mediante bases de datos obtenidas de redes sociales y otros lugares de la web que manejan nuestros datos.

Si se analiza todo lo anterior en conjunto, resulta evidente que para cualquier ciudadano resultaría a simple vista imposible saber si las cámaras de videovigilancia de un determinado lugar cuentan con la tecnología del reconocimiento facial o no. Evidentemente también surge la duda de si la aplicación de esta tecnología es realmente necesaria, puesto que el impacto sobre la privacidad de las personas resulta evidente. Pero todo esto se agrava si pensamos que el reconocimiento facial no solo implica en lo que respecta a su impacto sobre la privacidad identificar a la persona, también existe un impacto relacionado con la base de datos de la que se alimenta ese reconocimiento, quién tiene acceso a esa información, que se hace con ella y donde se almacenan los resultados. Así pues, el claro conflicto entre los beneficios que reportaría respecto a la seguridad podría en muchos casos no ser lo suficientemente claros al contraponerlos con el impacto que causa una tecnología de este estilo y todo lo que la rodea sobre el derecho a la privacidad de las personas.

En conclusión, la videovigilancia gracias a la tecnología del reconocimiento facial en tiempo real se enfrenta al reto de definir de forma clara los peligros que suponen para la privacidad y después, definir en qué casos prevalece el interés público y/o privado de garantizar la seguridad sobre el derecho a la privacidad de los ciudadanos.

Como en la mayoría de las ocasiones, son los legisladores y los jueces los que deben hacer esta valoración y por lo tanto no es extraño encontrar diferentes criterios de actuación en distintos lugares del mundo.

2.5.1 El caso chino

Uno de los casos más interesantes a la hora de analizar casi cualquier avance en sistemas de control y vigilancia es China. Este hecho, se debe fundamentalmente a dos razones. La primera, es que China es la segunda economía mundial y el desarrollo que ha experimentado en los últimos años no tiene comparación posible actualmente. Esto ha permitido desarrollar grandes ciudades equipadas con lo último en tecnología y por supuesto en vigilancia, con un mínimo impacto ya que se han ido instalando a la vez que sus principales ciudades crecen y evolucionan. La segunda, es que China desde 1949 y tras una guerra civil se rige por un gobierno totalitario. Esto, provoca entre otras cosas que no exista una separación de poderes y que por lo tanto ante cualquier conflicto frente al estado, prevalezca siempre este. Es decir, el problema de la privacidad frente a la seguridad en China siempre se inclinará hacia el derecho y deber de un estado de garantizar la seguridad.

Toda esta situación socio económica, se ve reforzada ante la clara apuesta del gobierno chino por la tecnología que ha llevado a varias empresas nacionales a situarse entre las líderes mundiales en el ámbito de la tecnología como puede ser el caso de Huawei, que actualmente está entre las empresas líderes en el sector de las telecomunicaciones.

Así pues, si mezclamos un gobierno autoritario, una economía potente y un país con una tasa de desarrollo de las más altas del mundo, obtenemos el coctel perfecto en el que desde el desarrollo hasta la aplicación de la tecnología sirven a los intereses del gobierno. De esta forma, hemos asistido a como China era una de las primeras potencias mundiales en imponer un férreo control a internet en su país, evitando aplicaciones webs y cualquier servicio que escapase al control y la censura china. Y si el control a sus propios ciudadanos llega incluso al ciberespacio, la vigilancia en la calle no podía ser menos.

La asociación de ideas entre seguridad y vigilancia es algo que viene de lejos y que en este trabajo ha salido varias veces. Por otro lado, ya se ha discutido las ventajas que han llevado a la implantación masiva de sistemas de videovigilancia, y la potencia que les otorgan los sistemas de reconocimiento facial en casi tiempo real. Si tenemos en cuenta todo esto junto con la casuística china, resulta evidente el porqué de que en China cuando se habla de seguridad, la palabra hipervigilancia esté intrínsicamente relacionada.

El uso del superlativo hiper en el caso de China no es baladí, puesto que si se quiere controlar a los ciudadanos de un país con una población estimada de 1.403.500.365 [30] cualquier sistema tiene que tener un tamaño desde en número de dispositivos, hasta en capacidad de computación de un orden de magnitud enorme. De hecho, se estima que en China existen unos 20 millones de cámaras según un artículo en The New York Times [31].

Con toda esta infraestructura masiva de cámaras desplegadas, China ya tenía resuelto el principal problema de un sistema de videovigilancia basado en reconocimiento facial, la instalación y distribución de las cámaras que alimentasen el sistema. Así pues, cuando hace unos años empezaron a poner en marcha en distintas ciudades del país los sistemas de videovigilancia, solo fue necesario reforzar el sistema de cámaras del que ya disponían.

Respecto del otro gran escollo que es la base de datos con la que comparar las imágenes de las cámaras, China cuenta con una base de datos de 90 terabytes con la fotografía e información personal de sus ciudadanos [32].

Así pues, el único problema que tenían los chinos era contar con un software lo suficientemente potente como para procesar todas estas imágenes en un tiempo muy reducido e identificar a la gente con un porcentaje lo suficientemente alto como para minimizar los falsos positivos. Para ello contaron con varias empresas chinas como Hisense, que actualmente controla el sistema en la ciudad de Qingdao [33], que fueron las encargadas de crear el software de reconocimiento facial. Esto, además, otorga la ventaja de que estas empresas pueden exportar sus sistemas a otros países generando beneficios para China y quien sabe si incluso acceso a los datos que generen estos programas.

Por último, en lo que respecta a los posibles problemas legales e incluso morales derivados de un sistema de videovigilancia de este estilo, recordemos que como ya se ha dicho, todo interés en China está supeditado al bien general del estado sin excepción.

De esta forma, China ha pasado a vigilar de forma activa a todos sus ciudadanos en lugares públicos, obteniendo resultados de esta iniciativa de forma casi inmediata. Estos resultados de los que hablo se traducen en la detención de más de 1.200 criminales en un año [33] gracias a que fueron detectados por el sistema de reconocimiento facial. De hecho, un reportero de la BBC comprobó la efectividad del sistema en 2017, siendo detenido en 7 minutos [34].

Dentro de China, merece especial mención la antigua colonia británica de Hong Kong, que desde el año 1997 en el que pasó a manos chinas se encuentra bajo un régimen de gobierno especial que pretende ir poco a poco integrándola en el sistema chino y por lo tanto vive una situación especial en la que poco a poco sus leyes se van adaptando a las de un estado totalitario. Es precisamente por uno de estos cambios en su sistema legal que ha desencadenado una larga serie de protestas y disturbios que Hong Kong se ha hecho famosa en el ámbito del reconocimiento facial puesto que, tras la reciente escalada de la violencia en las manifestaciones, los manifestantes están cubriendo sus rostros y destruyendo las cámaras de seguridad para evitar ser identificados por el reconocimiento facial [35]. Estos métodos se han demostrado bastante

efectivos y han llevado al gobierno a promulgar una ley que quiere prohibir el uso de prensas que oculten la cara [36].

En resumen, el caso chino, muestra una de las posibles soluciones al dilema de la seguridad frente a la privacidad para el reconocimiento facial, que en este caso se trata de la total subordinación de cualquier interés al bien del estado y, por lo tanto, el derecho a la seguridad colectiva que garantiza un estado estará siempre por encima del derecho de los individuos a la privacidad. Adicionalmente, este caso sirve para ver de primera mano un sistema total de reconocimiento facial con todo lo que ello implica tanto para bien como para mal.

Si bien el caso chino resulta muy interesante desde el aspecto legal y técnico, si lo que se pretende es intentar extrapolar el caso a Europa y más en concreto a España y relacionarlo con la RGPD, es quizás mucho más sencillo hacerlo con el caso de un país con un sistema de gobierno con mayores similitudes al nuestro como es el caso de Estados Unidos.

2.5.2 El caso de San Francisco

Dentro de Estados Unidos, es muy interesante el caso de San Francisco.

San Francisco, se vanagloria de ser la ciudad más tecnológica del mundo por ser sede desde hace pocos años de muchas de las empresas tecnológicas de Silicon Valley. Este hecho se debe fundamentalmente a dos factores, el primero es que es gran ciudad más cercana al Silicon Valley original y por lo tanto entraba dentro de la expansión natural por el norte. Y el segundo se debe a uno de los mayores inversores de EEUU, que en su día invirtió en empresas como Google o Twitter, Ron Conway [37].

Este inversor, al mudarse a San Francisco aprovechó para lanzar una web llamada sfciti.org, Con la que mediante iniciativas tecnológicas pretende mejorar la vida en la ciudad. Según un artículo de El País [37], 500 de las empresas que se trasladaron del valle a San Francisco formaban parte de esta web en 2013. Así pues, y gracias a la llegada de este inversor y de todas las empresas tecnológicas que llegaron después y se sumaron a la iniciativa de las soluciones tecnológicas para la ciudad, San Francisco se ha convertido en una de las ciudades más tecnológicas del mundo.

Teniendo en cuenta toda esta situación, es lógico pensar que San Francisco sirve de muestra al resto del mundo al estar a la vanguardia en la aplicación de la tecnología para mejorar y evolucionar una ciudad. Por eso, resulta sorprendente que, en el campo de la aplicación del reconocimiento facial para vigilar la ciudad, san Francisco se haya convertido en la primera gran ciudad de Estados Unidos en prohibir su uso [38]. Pero lo interesante de la prohibición son los argumentos que redactor de la norma Aaron Peskin, utiliza para justificarla.

> *“La normativa aprobada fue redactada por el supervisor Aaron Peskin, quien argumentó que el reconocimiento facial supondría un paso adelante hacia una mayor represión estatal. Durante el debate, Peskin puso como ejemplo a China y el empleo de dicha tecnología para mantener bajo control a algunas minorías musulmanas.” [38]*

Como se puede ver, Peskin habla de la mayor represión estatal que supone adoptar esta tecnología para la vigilancia y el uso de las fuerzas y cuerpos de seguridad, y nombra específicamente el caso de China. Así pues, resulta evidente que para los propios legisladores el reconocimiento facial en cámaras de videovigilancia supone un claro conflicto moral entre la seguridad y el derecho a la privacidad. Afortunadamente en el caso de San Francisco, los derechos de sus ciudadanos pesaron más que la promesa de seguridad que ofrece esta tecnología, pero esta postura está lejos de ser la Federal e incluso está alejada de la de otras ciudades de EEUU. Así por ejemplo se sabe que el FBI ya ha utilizado esta tecnología para realizar más de 390.000 búsquedas, o que el Servicio de Inmigración y Aduanas (ICE) recopiló fotografías de diversas agencias estatales de tráfico para identificar mediante el reconocimiento facial a inmigrantes sin papeles [39].

En resumen, a pesar de que la postura de San Francisco es novedosa al tratarse de la primera legislación clara y además en contra de la tecnología de reconocimiento facial, no parece indicar la tendencia general de Estados Unidos frente a esta tecnología ya que en otras ciudades e incluso a nivel federal, esta tecnología se usa. Es precisamente por todas estas causas que el debate en Estados Unidos está abierto y las posturas de detractores y gente a favor hacen que sea muy interesante estar atentos a lo que se dice y se hace a este respecto.

Si bien hasta ahora se han visto dos casos bastante enfrentados en la forma de enfrentarse al reconocimiento facial que nos pueden permitir imaginar cómo sería adoptar una posición u otra, ninguno contaba con el contexto que cuenta Europa y en especial España con la introducción de la RGPD.

2.5.3 España, RGPD y reconocimiento facial

En España cada vez son más frecuentes los ejemplos de uso del reconocimiento facial, aunque siempre para aspectos no relacionados con la vigilancia. Por ejemplo, el aeropuerto de Menorca cuenta desde hace un tiempo con un sistema de reconocimiento facial para acceder a la zona de embarque y al avión. Pero si es cierto que existe un ejemplo que ha pasado ciertamente desapercibido de uso del reconocimiento facial en sistemas de videovigilancia en nuestro país.

En concreto, me refiero a la estación de autobuses sur de Madrid. Esta estación que es la más grande de Europa para autobuses de largo recorrido y que cuenta con 20 millones de transeúntes al año, fue pionera en 2015 al realizar una remodelación en la que la seguridad fue clave. En ella, se instalaron cámaras IP de alta resolución compatibles con la tecnología de reconocimiento facial. En total, 12 de las 100 cámaras con las que cuenta la estación son compatibles.

Toda esta revolución que sufrió la estación ha provocado que la estación pase de 5 incidentes diarios a 5 al mes [40]. Aunque el jefe de seguridad de la estación y promotor de esta gran reforma quitaba merito al reconocimiento facial y se lo daba a otras causas como el aumento de vigilantes en unas declaraciones de 2016.

> *"En un principio queríamos usar el reconocimiento facial para reducir los hurtos en la estación, pero este problema se solucionó de forma natural con un incremento de la vigilancia física…" [41]*

De todas formas, la estación ha encontrado un uso a este sistema como el propio jefe de seguridad, Miguel Ángel Gallego, comentaba.

> *"Por ello hemos aplicado esta tecnología a la lucha contra el terrorismo, el tráfico de drogas, la trata de humanos o la búsqueda de desaparecidos…Siempre lo hacemos a requerimiento de los jueces, la Policía Nacional o la Guardia Civil" [41]*

Así pues, la estación de Méndez Álvaro como es popularmente conocida ha pasado a ser el primer caso de videovigilancia de un espacio público llevado por una empresa privada con la colaboración del estado que el que el principal suministrador de sospechosos a buscar por el sistema.

Como ya hemos visto, las leyes españolas prevén el uso de la videovigilancia siempre y cuando se cuente con la debida autorización y si anuncie mediante carteles u otros métodos. Ahora bien, sobre el uso de sistemas de reconocimiento facial que complementen el sistema no se dice nada claramente, aunque se puede sobreentender con lo visto hasta ahora que, a la hora de justificar el uso del sistema de videovigilancia, el uso de un sistema de reconocimiento facial también debe ser informado y por lo tanto entrar en la valoración del conjunto para su aprobación. No obstante, la RGPD sí que hace referencia al tratamiento de los datos y en especial a los de carácter biométrico como son los empleados en este caso, y que los incluye en una categoría de especial protección. En concreto su artículo 9.1 la RGPD dice que:

> *"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a*

identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física." [1]

Ahora bien, la propia RGPD se encarga de añadir una excepción a este artículo para garantizar que las fuerzas y cuerpos de seguridad de un estado puedan usar estos datos en el ejercicio de sus funciones o si la persona da expresamente su consentimiento.

"2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

…

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;" [1]

No obstante, la propia RGPD también indica que esta excepción en aras del interés público debe ser proporcional y respetar y proteger los derechos y la privacidad de las personas afectadas.

Así pues, el caso de uso de la videovigilancia en la estación de Méndez Álvaro quedaría al amparo de esta excepción puesto que se usa por un bien de interés público que es el de garantizar la seguridad en una zona de especial riesgo y además solo se usa bajo requerimiento judicial o de alguna de las fuerzas y cuerpos de seguridad del estado, por lo que siempre queda constancia social.

Aunque como se desprende de las declaraciones del señor Gallego no siempre se hace bajo un requerimiento oficial, sino que a veces colaboran de forma informal con la policía.

"…aunque Gallego confirma que en muchos casos también colaboran de forma informal con los cuerpos policiales." [41]

Esta última revelación no hace más que recalcar los peligros de la tecnología de reconocimiento facial, puesto que se está admitiendo un uso como mínimo de dudosa moralidad de esta tecnología y además pone de manifiesto la facilidad con la que se puede hacer un mal uso de esta tecnología sin que quede ni constancia ni tenga consecuencias sobre los responsables de la misma.

En cualquier caso, y pese al ejemplo de Méndez Álvaro, España parece estar todavía lejos de que la tecnología de reconocimiento facial se generalice dentro de la videovigilancia a pesar de que ya se empieza a extender su uso a lugares como IFEMA. No obstante, el ejemplo también pone de manifiesto la facilidad y la frivolidad con al que se implementa y maneja esta tecnología a día de hoy en nuestro país.

Con esto, se puede dar por cubierta de forma general la situación actual de la videovigilancia y el reconocimiento facial en el mundo. Además, con lo visto anteriormente en tema de regulación tanto a nivel nacional con las distintas leyes y a nivel europeo con la RGPD, y con los antecedentes históricos que nos permiten saber de dónde venimos y por qué estamos en la situación que estamos actualmente, se ha cubierto de forma bastante completa el conflicto existente desde hace años entre privacidad y seguridad.

Hasta esta aproximación del contenido y desarrollo de este trabajo de fin de máster. Y teniendo en cuenta la experiencia estudiada correspondiente a la evolución del derecho a la privacidad, la tecnología y la legislación a lo largo de la historia, he establecido una serie de conclusiones que se pasan a exponer.

3. Conclusiones

El conflicto entre el legítimo derecho de los estados a garantizar la seguridad y el derecho a la privacidad de las personas no es un tema nuevo, pero los constantes avances en tecnología, los recientes escándalos que han salido a la luz sobre el uso que se hace de datos personales y sobre todo la nueva legislación europea de protección de datos han hecho necesaria una revisión de este conflicto, y aunque ya se ha escrito y se sigue escribiendo sobre este asunto y sus implicaciones, aún quedan flecos sobre los que poco o nada se ha discutido.

Uno de ellos, es la aparición de sistemas de reconocimiento facial prácticamente instantáneos que se están implementando en cámaras de videovigilancia. Estos sistemas prometen incrementar la seguridad de forma exponencial, pero el impacto que tienen sobre la privacidad tanto por lo que implica tratar la imagen de una persona como por la base de la que se alimenta este sistema de reconocimiento, no es precisamente trivial. Es decir, estamos ante una tecnología que impacta de forma muy significativamente en ambos lados de la balanza y de la que por ahora no se ha hablado demasiado en nuestro país.

De esta forma, este trabajo ha pretendido analizar esta problemática comparándola con casos conocidos y enfrentándola a lo que la actual legislación regula al respecto.

Así pues, se puede concluir que:

1. **El 11S supuso un antes y un después para el conflicto entre la seguridad y la privacidad, que provocó una oleada de reacciones de los estados que supusieron un gran retroceso del derecho a la privacidad, así como de claros abusos en el uso de información.**

   Tras los atentados del 11S y los de años posteriores en Europa el miedo a los terroristas se propagó alentado por los estados, lo cual les dio carta blanca para acometer reformas en la legislación que consagraban el derecho del estado a prevenir nuevos ataques. Esto supuso un claro retroceso para el derecho a la privacidad y llevó a claros abusos como los destapados por Snowden.

2. **Los diversos escándalos en el uso de datos personales destapados en los últimos años y que afecta tanto a estados como empresas privadas, han provocado la indignación popular y la consiguiente reacción de algunos legisladores que están empezando a legislar para proteger los datos personales.**

   Las revelaciones hechas por Snowden y otros exagentes de diferentes agencias americanas, han puesto ante los focos las distintas tácticas de los estados para recolectar, analizar e intercambiar información de

sus propios ciudadanos, así como la información de la que recolectan diferentes empresas privadas y la impunidad con la que manejaban e intercambiaban estos datos. Esto ha provocado la indignación de la población y de algunos legisladores, que ante todo esto están promoviendo iniciativas como la RGPD para intentar controlar por lo menos el uso que se hace de la información personal que recolectan las empresas.

3. **La evolución de la tecnología ha provocado el crecimiento exponencial de la información creada, pero también, la aparición de nuevas tecnologías y el perfeccionamiento de algunas viejas que han facilitado y creado nuevas oportunidades para recolectar y tratar esta información.**

   Desde el inicio de la era de la información, la cantidad de datos creados por el hombre no ha parado de crecer de forma casi exponencial. Esto, junto con el hecho de que esta información incluye muchísimos datos de carácter personal generados por millones de personas, ha despertado el interés de empresas y estados, que han visto la oportunidad perfecta de recolectar información tanto de individuos como de colectivos sin apenas esfuerzo y sin resultar especialmente invasivos puesto que es el propio usuario el que facilita la información. Esto ha provocado la proliferación de tecnologías y metodologías para mejorar el tratamiento de estos datos tanto en lo referente al tiempo de procesamiento como la granularidad y nivel de acierto de los resultados obtenidos.

4. **Los usuarios no son conscientes de los datos personales que entregan ni del uso que las empresas hacen de ellos.**

   Aunque la RGPD ha mejorado la información que se pone a disposición de los usuarios sobre los datos que se recolectan y el uso que se hace de ellos, existen estudios que ponen de manifiesto que es imposible que una persona se lea todas las políticas de privacidad de los sitios web que utiliza, por lo que al final lo más común es aceptar dichas políticas sin leerlas.

5. **Las expectativas a medio y largo plazo son que la cantidad de datos personales que damos aumente junto con el tratamiento que se hace de los mismos.**

   Las nuevas tecnologías como el llamado IoT que va muy ligado al concepto de Smart City, se basan en la recolección de cada vez más datos y en el análisis que se hace de estos en su conjunto, por lo que la tendencia de los últimos años que nos lleva a un mundo cada vez más conectado y automatizado conlleva también el dar cada vez más datos personales y autorizar su tratamiento para acceder a las ventajas que ofrecen estas tecnologías.

6. **La video videovigilancia, aunque es una tecnología ya antigua, está cobrando cada vez más importancia gracias al abaratamiento de precios y a su combinación con otras tecnologías como el reconocimiento facial**.

   La videovigilancia es una tecnología ya conocida y tan aceptada y extendía que ya forma parte del paisaje urbano de casi cualquier ciudad. Tanto es así que cuenta con legislación específica desde hace años sobre cuándo y cómo se debe usar tanto en el ámbito privado como el público. Ahora bien, el abaratamiento de esta tecnología que ha hecho posible que todo el mundo tenga su propia cámara de videovigilancia, como su combinación con otras tecnologías como el reconocimiento fácil, están haciendo que proliferen cada vez más y por lo tanto supongan un nuevo reto para la privacidad.

7. **La videovigilancia en España en lugares públicos está regulada mediante una legislación bastante garantista, aunque siempre depende la autorización de un juez o la autoridad competente y por lo tanto está abierta a interpretación**.

   Las leyes españolas respecto a la videovigilancia son bastante garantistas ya que anteponen siempre conceptos como la idoneidad y proporcionalidad. Es decir, se debe evitar el uso de cámaras siempre que el impacto sobre las libertades individuales sea mayor que el beneficio obtenido. Aun así, este balance queda en manos de un juez que es el que debe decidir de qué lado se inclina la balanza y aceptar o denegar el uso de cámaras.

8. **La RGPD introduce aspectos garantistas en cuanto al tratamiento y protección de los datos, y deja abierta explícitamente la puerta a que los cuerpos y fuerzas de seguridad pueden saltarse algunas limitaciones de esta regulación si actúan por el bien de la sociedad.**

   La RGPD, ha incluido aspectos interesantes en la videovigilancia como el que garantiza que se considere tratamiento de datos personales a las cámaras que recogen imágenes, pero no las graban. Y adicionalmente ha incluido garantías respecto al uso que de los datos obtenidos se pueden hacer y respecto al deber de informar sobre qué datos y para qué se usan. No obstante, artículos como el 6.1 que garantiza el tratamiento de datos si se realiza por motivos de bien de interés público por parte de los cuerpos y fuerzas de seguridad, hacen que en un país como España en el que la videovigilancia en lugares públicos está solo permitida al estado, esta legislación pierda fundamento.

9. **Los avances en reconocimiento facial y su implementación en sistemas de videovigilancia suponen un gran avance en seguridad, pero también un gran riesgo para la privacidad.**

   Desde hace unos años los avances en sistemas de reconocimiento facial y tratamiento masico de datos, han conseguido que sea posible identificar a una persona en cuestión de segundos. Esto en conjunto con las cámaras de videovigilancia podría permitir a la policía localizar delincuentes y rastrearlos dentro de una ciudad en cuestión de segundos y atraparlo en cosa de minutos. Ahora bien, las dudas respecto al impacto en la privacidad de los ciudadanos son evidentes ¿De dónde sale la base de datos con caras y nombres? ¿Quién maneja el sistema? ¿Qué se hace con los resultados de la identificación en tiempo real? ¿Se almacenan? ¿Durante cuánto tiempo?

10. **Este dilema ya está encontrado soluciones diversas en diferentes países e incluso dentro de un mismo país.**

    Los casos de China y estados unidos y más concretamente de la ciudad de San Francisco, ponen de relieve las diferentes formas de enfrentarse a este nuevo dilema que ha puesto sobre la mesa la tecnología del reconocimiento facial aplicada a la videovigilancia. Así pues, los estados y ciudades deben decidir nuevamente si el benéfico en seguridad pesa más que el impacto sobre la privacidad.

11. **Este dilema ya ha llegado a España y aunque la legislación española parece bastante garantista, los malos usos que se pueden hacer con esta tecnología deberían provocar una revisión de las leyes.**

    El caso de la estación de Méndez Álvaro en Madrid pone de manifiesto que en España el dilema de la videovigilancia con reconocimiento facial está aquí para quedarse. Pero además tal y como el responsable de la estación admite sin ser aparentemente muy consciente de lo que dice, la facilidad con la que se puede hacer un mal uso de esta tecnología aun teniendo la mejor de las intenciones es ciertamente alarmante.

4. Glosario

11S: 11 de septiembre de 2001. Fecha de los atentados contra las torres gemelas de Nueva York.

5G: Quinta generación de las comunicaciones móviles, que supone un gran cambio tanto a nivel estructural como de prestaciones respecto a sus predecesoras. Entre otras cosas se caracteriza por una muy baja latencia.

Cámaras IP: Cámara que incluye un pequeño procesador el cual se usa genéricamente para enviar imágenes de video por internet.

Datos personales: Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal. [42]

IoT: Internet de las cosas. Este concepto se refiere a la conexión a internet de objetos cotidianos como lavadoras, neveras, zapatillas etc.

PRISM: Programa espía usado por la NSA para recolectar información de comunicaciones de usuarios de empresas como Google, Facebook, Apple o Microsoft.

Redes neuronales: Modelo de computación formado por multitud de nodos conectados entre sí.

RGPD: Reglamento General de Protección de Datos.

Smart City: Representa el concepto de una ciudad en la que todos sus elementos desde el mobiliario urbano hasta las personas están conectados e intercambian información en aras de la eficiencia y el bienestar tanto individual como colectivo.

5. Bibliografía

[1] Unión Europea. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[2] Constitución Española. Boletín Oficial del Estado, 29 de diciembre de 1978, núm. 311.

[3] España. 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. Boletín Oficial del Estado, 5 de agosto, núm. 186.

[4] España. Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de 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. Boletín Oficial del Estado, 19 de abril, núm. 93.

[5] España. Ley 5/2014, de 4 de abril, de Seguridad Privada. Boletín Oficial del Estado, 5 de abril, núm. 83.

[6] España. Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado, 14 de diciembre, núm. 298.

[7] España. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado, 17 de septiembre, núm. 260.

[8] España. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre, núm. 294

[9] W. Bush, G. (2003). *Discurso íntegro del ultimátum de George W. Bush a Sadam Husein*. El País. Recuperado de: https://elpais.com/elpais/2003/03/18/actualidad/1047977036_850215.html

[10] W. Bush, G. (2001). *Discurso: 11 de septiembre de 2001.* Wikisource. Disponible en: https://es.wikisource.org/wiki/Discurso:_11_de_septiembre_de_2001

[11] Johnson, L. (2013). *George W. Bush Defends PRISM: 'I Put That Program In Place To Protect The Country'*. Huffington Post. Recuperado de:https://www.huffpost.com/entry/george-bush-prism_n_3528249?guce_referrer=aHR0cHM6Ly9lcy53aWtpcGVkaWEub

3JnLw&guce_referrer_sig=AQAAAB_kyQZMoynNyyurn2o6ac8o6XsJBACXqwZnlJc0T-MeJNy9m7-lLHP-hvNVWBPH_2XD_6gOWJ9b8LqdyGfZFwXG-apK8xX9yfJmx7zqKoQByH_hDZepsy9WdpOJPmXxJvjGq705H8MiO3wUwTWqIJrN9PpHoDNJyY_T7-ASguW3&_guc_consent_skip=1574620968

[12] B. Lee, T. (2013) *How Congress unknowingly legalized PRISM in 2007*. The Washington Post. Recuperado de: https://www.washingtonpost.com/news/wonk/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/

[13] Gellman, B. y Poitras, L. (2013) *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. The Washington Post. Recuperado de: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?noredirect=on

[14] Reinsel, D., Gantz, J., & Rydning, J. (2018, noviembre). *The Digitization of the World*. Recuperado de https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

[15] We Are Social, & Hootsuite. (2019, 30 enero). *Digital 2019: Global Internet Use Accelerates - We Are Social*. Recuperado de https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

[16] Llaneza, P. (2019). *Datanomics: Todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*. Deusto Editorial Planeta.

[17] M. Mcdonald, A. & Faith Cranor, L. (2008). *The Cost of Reading Privacy Policies*. I/S: A Journal of Law and Policy for the Information Society, vol. 4m nº3, pp. 543-568. Ohio State University. Motriz College of Law. Recuperado de https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf

[18] Ruiz, J. J. (2017, 18 diciembre). *Varias vulnerabilidades en cámaras IP Zivif*. Una al Día. Recuperado de https://unaaldia.hispasec.com/2017/12/varias-vulnerabilidades-en-camaras-ip-zivif.html

[19] Goldman, J. (2012, 1 noviembre). *Most U.S. Drone Feeds Aren't Encrypted*. eSecurity Planet. Recuperado de https://www.esecurityplanet.com/network-security/most-u.s.-drone-feeds-arent-encrypted.html

[20] Agencia española de protección de datos. (s.f.). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*. Recuperado de https://www.aepd.es/media/guias/guia-videovigilancia.pdf

[21] Agencia española de protección de datos. (s.f.). *Videovigilancia*. Recuperado de https://www.aepd.es/areas/videovigilancia/index.html

[22] España. Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de 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. Boletín Oficial del Estado, 19 de abril de 1999, núm. 93.

[23] España. Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte. Boletín Oficial del Estado, 12 de julio de 2007, núm. 166.

[24] Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte. Boletín Oficial del Estado, 9 de marzo de 2010, núm. 59.

[25] Agencia española de protección de datos. (s.f.). *Videovigilancia en tiempo real*. Recuperado de https://www.aepd.es/media/informes/informe-juridico-rgpd-videovigilancia-tiempo-real.pdf

[26] Agencia española de protección de datos. (s.f.). *Cámaras en tiempo real*. Recuperado de https://www.aepd.es/media/informes/informe-juridico-rgpd-camaras-en-tiempo-real.pdf

[27] Agencia española de protección de datos. (s.f.). *Drones*. Recuperado de https://www.aepd.es/media/informes/informe-juridico-rgpd-drones.pdf

[28] Agencia española de protección de datos. (s.f.). *Responsabilidad proactiva*. Recuperado de https://www.aepd.es/reglamento/cumplimiento/principio-responsabilidad-proactiva.html

[29] Unión Europea. 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, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[30] Naciones Unidas. (2019). *World Population Prospects 2019*. Recuperado de https://population.un.org/wpp/DataQuery/

[31] Mozur, P. (2018, 8 julio). *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*. The New York Times. Recuperado de https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html

[32] Stephe, C. (2017, 12 octubre). *China to build giant facial recognition database to identify any citizen within seconds*. South China Morning Post. Recuperado de https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any

[33] Araújo, S. (2017, 15 diciembre). *Miles de cámaras te vigilan: comprobamos cómo funciona el colosal sistema de videovigilancia en China*. Xataka. Recuperado de https://www.xataka.com/privacidad/miles-de-camaras-te-vigilan-el-colosal-sistema-de-videovigilancia-en-china

[34] Sudworth, J. (2017). *El asombroso sistema de videovigilancia en China que detectó a un reportero de la BBC en tan solo 7 minutos. BBC*. Recuperado de https://www.bbc.com/mundo/media-42358019

[35] Agencias. (2019, 25 agosto). *Los manifestantes de Hong Kong tumban torres de reconocimiento facial y la Policía les lanza gases lacrimógenos*. The Huffington Post. Recuperado de https://www.huffingtonpost.es/entry/los-manifestantes-de-hong-kong-tumban-torres-de-reconocimiento-facial-y-la-policia-les-lanza-gases-lacrimogenos_es_5d62622de4b02cc97c8f0793

[36] Arana, I. (2019, 4 octubre). *Hong Kong invoca una ley de emergencia para prohibir las máscaras en las protestas*. La Vanguardia. Recuperado de https://www.lavanguardia.com/internacional/20191004/47795423260/hong-kong-ley-emergencia-prohibir-mascaras-protestas.html

[37] Cobo, V. (2013, 28 abril). *San Francisco se destapa como la capital tecnológica del mundo*. El País. Recuperado de https://elpais.com/internacional/2013/04/26/actualidad/1366930791_855552.html

[38] Mendoza, S. (2019, 15 mayo). *San Francisco, primera ciudad en prohibir la tecnología de reconocimiento facial en EE UU*. El País. Recuperado de https://elpais.com/tecnologia/2019/05/15/actualidad/1557904606_766075.html

[39] EFE. (2019, 8 julio). *EE.UU. aplica reconocimiento facial en licencias para hallar a indocumentados*. EFE. Recuperado de https://www.efe.com/efe/america/sociedad/ee-uu-aplica-reconocimiento-facial-en-licencias-para-hallar-a-indocumentados/20000013-4018545

[40] Axis Communications. (2016). *Estación sur de Autobuses de Madrid: Análisis de vídeo para la estación de autobuses con más tránsito de Europa*. Axis. Recuperado de https://www.axis.com/files/success_stories/ss_trn_south_madrid_busstation_67720_es_1607_lo.pdf

[41] Iglesias Fraga, A. (2016, 3 mayo). *'Gran Hermano' en la estación de bus que ve a terroristas y desaparecidos*. El Mundo. Recuperado de https://www.elmundo.es/economia/2016/05/03/57285fbc468aeba9518b45d5.html

[42] Comisión europea. (s.f.). *¿Qué son los datos personales?* Comisión europea. Recuperado de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

[43] Agencia española de protección de datos. (s.f.). *Drones y Protección de Datos*. Recuperado de https://www.aepd.es/media/guias/guia-drones.pdf