ESCUELA INTERNACIONAL DE DOCTORADO
Programa de Doctorado en Ciencias Sociales

Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia

Autor:
D. Juan José Delgado Morán

Director:
Dr. D. Cesar Augusto Giner Alegría

Murcia, septiembre 2018

ESCUELA INTERNACIONAL DE DOCTORADO
Programa de Doctorado en Ciencias Sociales

Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia

Autor:
D. Juan José Delgado Morán

Director:
Dr. D. Cesar Giner Alegría

Murcia, septiembre 2018

UCAM

UNIVERSIDAD CATÓLICA
DE MURCIA

AUTORIZACIÓN DEL DIRECTOR DE LA TESIS PARA SU PRESENTACIÓN

El Dr. D. César Augusto Giner Alegría como Director[1] de la Tesis Doctoral titulada "Sociedad de Control y Panóptico Electrónico. La Victima de la Videovigilancia" realizada por D. Juan José Delgado Morán en el Departamento de Ciencias Sociales, **autoriza su presentación a trámite** dado que reúne las condiciones necesarias para su defensa.

Lo que firmo, para dar cumplimiento a los Reales Decretos 99/2011, 1393/2007, 56/2005 y 778/98, en Murcia a 15 de julio de 2018.

RESUMEN

Esta tesis se ocupa de aquellos derechos que garantizan la Protección de Datos frente al poder del Estado, reconocidos en el texto de nuestra Constitución y en la Declaración Universal de los Derechos Humanos. El presente estudio revisa la evolución de las legislaciones relativas a la privacidad y la protección de datos en España en intima consonancia con Europa y la legislación comunitaria. Presentando esta evolución que se sucede a lo largo de los años dados los avances de la técnica que suponen desde la aprobación del Convenio 108 hasta el Derecho al Olvido. Nos meteremos de lleno en las garantías constitucionales respecto al tema que nos trata, profundizando en los límites temporales y en los derechos de los mismos. Abordaremos la protección de datos en supuestos especiales, y concluiremos este estudio profundizando en las recomendaciones internacionales en dicha materia.

Palabras Clave: *Datos personales; Derechos Humanos; Derecho a la Información; Medidas de seguridad; Protección de datos.*

ABSTRACT

This work will address those rights that ensure the protection of data against the power of the State, recognized in the text of our Constitution and the Universal Declaration of human rights. We put us squarely in the constitutional guarantees regarding the issue that us deals, deepening in the time limits and on the rights of the same. We will address the protection of data in special cases, and conclude this study delving into the international recommendations in this field.

Key Words: *Personal data, Human rights; Right to information; Safety measures; Data protection.*

Contenido

AGRADECIMIENTOS

A mi padre que me enseño que con dedicación y entusiasmo se puede llegar hasta donde uno quiera. A Daniela mi hija, por irse antes de tiempo. Me enseñaste que, como tú, todo es efímero, antes o después, incluido este trabajo, muy a pesar de que siempre permanezcas en mi pensamiento.

A quienes comparten conmigo el presente: a mi Madre, con sus todavía desvelos por nosotros, a Lenny, mi mujer y mi luz, a Valeria mi alegría y dedicación, y a Alejandro que acabas de llegar, mi futuro y esperanza. Todos ellos, el sino de mis esfuerzos, que son sin embargo, tareas gratas para lograr vuestra sonrisa.

A mis amigos, a mis maestros, a mis estudiantes, a mis condiscípulos y a mis compañeros de trabajo de todos los tiempos. A quienes me acompañaron en este proceso y me dieron ánimo para iniciarlo, pero, sobre todo, para terminarlo. Por todos ellos he decidido apartarme de la crítica y tratar humildemente y de manera constructiva, hacer un aporte simple a la ciencia del derecho y de la criminología.

Para quienes vengan y crean que el futuro siempre será mejor y encuentren en este trabajo la inspiración para nuevas investigaciones y aportes al sistema de derechos que nos amparan, aunque cada vez parezcan menos.

Muchas personas han trabajado conmigo en esta Tesis, a ellos mil y mil gracias por sus aportes y paciencia. Especial reconocimiento a mi maestro, Cesar Giner Alegría, ya que, sin su cariño, y empatía, comprensión

y ánimo, su esfuerzo, su tesón, y su confianza en mí, no hubiera podido ser posible la culminación de la tarea.

Y como no a los expertos en los temas tratados, que me permitieron caminar a hombros de gigantes, ya que de sus publicaciones y enseñanzas pude extraer lo mejor de su sapiencia y con ello construir mi aporte.

Gracias a Dios por darme fuerzas para llevar a cabo esta azarosa empresa.

I

INTRODUCCIÓN

I.INTRODUCCIÓN

La investigación que se presenta, trata de un estudio jurídico de la vigilancia masiva y la afectación de los derechos de intimidad, secreto a las comunicaciones y la protección de las personas frente al tratamiento de sus datos personales. Ciertamente, los avances de las tecnologías, en los últimos años, han transformado a los seres humanos en muchos sentidos y han permitido un progreso sin precedentes. La sociedad contemporánea depende en muchos aspectos de las facilidades ofrecidas por las nuevas Tecnologías de Información y Comunicación. La interconectividad ha generado el acceso a la mayor parte de la población mundial, a una vastísima y variada cantidad de información, acortando los límites espaciales y temporales. Uno de los grandes inventos en este campo es la red Internet, que sin duda ha permitido y facilitado importantes cambios políticos, económicos y sociales.

A través de la historia han ocurrido hechos relacionados con la vigilancia indiscriminada y arbitraria, sin embargo, de forma reciente se ha revelado la utilización de un nuevo tipo de vigilancia, la vigilancia electrónica, tema que de reciente data inició un gran debate en la academia y diversos sectores de la sociedad. Es así como, a pesar de las considerables ventajas que representan estas nuevas tecnologías, también han aparecido nuevos problemas y desafíos que causan preocupación en la población. Internet ha actuado como un potenciador de las conductas de las personas con un efecto multiplicador. De esta manera, los derechos y libertades fundamentales se han visto afectados de forma positiva y negativa. Contenido de la investigación. Inicialmente se planteó un estudio sobre el origen histórico de los derechos que se suponen vulnerados y sobre la evolución histórica de esos derechos ante el creciente uso y actualización de las tecnologías de información y comunicación.

Para ello, se plantea un análisis doctrinal, normativo y jurisprudencial de los derechos relacionados con los derechos de intimidad y privacidad. Uno de los derechos más afectados por el uso de las tecnologías de información y comunicación ha sido el derecho de intimidad de las personas. Este derecho se ha visto vulnerado por diversas conductas de los gobiernos, las empresas y personas particulares.

La presente investigación se propone analizar una de estas conductas, particularmente la vigilancia masiva, y su afectación a los derechos fundamentales

de las personas, en especial la que produce a los derechos de intimidad, el secreto a las comunicaciones y la protección de los datos personales. De esta manera, se exponen los retos jurídicos que enfrentan los sistemas de protección de los derechos fundamentales y se identifican los problemas relacionados con la protección del derecho a la intimidad en la sociedad contemporánea para abordar el tema de la vigilancia masiva como herramienta utilizada por parte de los gobiernos tecnológicamente avanzados. El derecho a la intimidad se ha visto afectado de forma considerable ante la permanente utilización y globalización de las tecnologías, lo que ha provocado la necesaria adaptación o evolución de este derecho a efectos de continuar con la vigencia y defensa de los derechos de las personas. La aparición de Internet supone un desafío a los operadores del derecho, situación que ha motivado una constante actividad a fin de proponer un marco jurídico que regule ciertas actividades que ocurren en los entornos virtuales. Los gobiernos también se han beneficiado con la utilización de estas tecnologías permitiendo una mejora considerable en la atención de sus fines y objetivos.

Sin embargo, estos también han aprovechado dichas tecnologías, particularmente la vigilancia electrónica, para combatir el terrorismo y otros delitos, sin embargo, al utilizar estas técnicas se termina también afectando la intimidad y la privacidad de las personas. La actividad desplegada por algunas agencias de inteligencia pareciera que se ha desarrollado con base en una cuestionable legislación adoptada ante la urgencia y necesidad de combatir actos terroristas, lo que ha permitido el acceso a las comunicaciones y los documentos privados de las personas con el objetivo de proteger la seguridad interna de las naciones, en la investigación se realiza un análisis y sistematización de la normativa que funciona como sustento de las actividades de las agencias de inteligencia y se analiza la nueva normativa en la cual se trató de reducir el impacto que tienen esas actividades en la vida privada de las personas.

Estos procesos, cada vez más agudos, tratan de delimitar, a través de la actividad administrativa y jurisdiccional, los límites de las informaciones y datos a los cuales pueden tener acceso las personas. De una parte, se presenta el derecho al acceso a la información pública, que se traduce en un principio o regla general y como excepción se presenta entonces, la otra parte, que protege el acceso a la información que está reservada a las personas por tratarse de asuntos que son parte de su vida privada. Indudablemente, se aprecia como la vigilancia masiva

nace como respuesta a los ataques y peligros contra la seguridad nacional, con la utilización de tecnologías que permiten a los gobiernos escuchar las llamadas telefónicas, escanear las redes de datos, leer correos electrónicos y mensajes de texto, seguimiento de personas, etc.

Sin embargo, aunque el empleo de las técnicas de la vigilancia electrónica, se presenta como una de las mejores soluciones, para combatir el terrorismo, evitar los conflictos sociales y proteger la seguridad nacional de los Estados a nivel internacional, la crítica principal a la utilización de esta técnica, radica en el hecho de que la vigilancia masiva no discrimina a los sujetos investigados y recae en una gran parte de la población civil que no está involucrada en actividades ilícitas lo que afecta, consecuentemente, los derechos fundamentales, civiles y políticos de la población en general.

Tratar de determinar si con el afán de crear sociedades más seguras, es necesario renunciar a la intimidad y, de ser así, establecer cuáles podrían ser los límites y las medidas necesarias para protegerse ante los posibles excesos o abusos. Se advierte como la protección jurídica de la intimidad, aunque muy importante, pareciera no ser una completa solución para la protección de los datos e intimidad de las personas, al menos de los datos compartidos en Internet.

Los límites de jurisdicción territorial, la falta de personalidad, la gran capacidad de almacenamiento, el constante avance y refinamiento de tecnologías que facilitan la vigilancia y el interés económico, podrían ser algunas de las causas que impiden una adecuada protección. La tutela de este derecho ha generado la creación de agencias de protección de datos, las que, mediante procedimientos administrativos, se han convertido en la primera línea de defensa y protección de los datos de las personas. Asimismo, se estima que los ámbitos de intimidad y privacidad han cambiado. Las personas ya no son tan privadas ni tan íntimas como cuando no existían las avanzadas tecnologías y las facilidades de acceder a la información, en especial la que se considera de carácter público. Entre los problemas generados con el uso de estas tecnologías está la seguridad informática, por las inmensas posibilidades que se ofrecen en la red de redes dando pie a que aparezcan los peligros. Esto plantea serios retos a la ciencia jurídica, pues el derecho no puede constituir un obstáculo para el desarrollo de las nuevas tecnologías, ni tampoco puede convertirse en un obstáculo.

Pero por otro lado, la ciencia jurídica afronta el reto de tutelar la frágil

situación en la que se encuentran los derechos de privacidad e intimidad de las personas ante el gran desarrollo de las nuevas tecnologías, y su amplia e ilimitada capacidad que tienen para atentar contra esos derechos, con el agravante de que las respuestas jurídicas han sido muy fraccionadas o regionales, limitadas por las fronteras nacionales, a diferencia del ámbito global en que se desenvuelven dichas tecnologías y las empresas que las respaldan.

Si bien los derechos fundamentales, como todos los derechos, pueden ser limitados, sin embargo, estas limitaciones deben ser legítimas, necesarias, razonables y proporcionadas, de manera que estén dispuestas por ley, sean claras y limitadas. Se estima que una persona bajo vigilancia ya no es libre y una sociedad bajo vigilancia ya no es una democracia. Para mantener la validez de los derechos fundamentales, deben aplicarse todos los derechos democráticos en el entorno virtual como en el espacio real. Es indudable que los intereses particulares ceden ante los intereses colectivos, sin embargo, en los casos de vigilancia electrónica masiva los derechos afectados son los de una colectividad.

Si la seguridad de un Estado se encuentra en peligro y corre un riesgo inminente la nación, la integridad territorial o la independencia política, sería justificable la utilización de medidas que puedan desplazar o minimizar los derechos de las personas. Ahora bien, en el momento en que esas medidas no sean necesarias, deberán restituirse los derechos que fueron suspendidos, regresando la situación a su protección original. Si bien se reconoce que todo individuo tiene derecho a la seguridad, también tiene derecho a no ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, de manera que sólo ante casos excepcionales, debidamente previstos en la ley, podrían admitirse limitaciones. Estos derechos son reconocidos por tener una carga de protección del mismo grado, pues en ambos casos existe un interés general o colectivo, si se atiende a que la afectación al derecho de intimidad repercute de forma negativa en millones de personas, incluyendo tanto a nacionales como a extranjeros. Las revelaciones sobre la existencia de la vigilancia masiva deben ensanchar el panorama y atraer la atención de las personas a dos cosas: la primera, que toda actividad electrónica está o puede ser vigilada y; la segunda, que toda la información colectada puede ser ilegalmente sustraída.

Sin duda alguna, seguirán apareciendo nuevos retos que podrán a prueba los mecanismos de protección de la intimidad y los datos. Por lo anterior, resulta

necesario que se fortalezcan los mecanismos existentes y se creen nuevas formas de protección de los datos de las personas, así como se instauren programas permanentes para la revisión de los mecanismos y las agencias de protección. Desde luego es prácticamente inviable una postura rígida que impida la vigilancia masiva y el análisis de datos existentes en Internet. Por ello se estima importante que exista una adecuada regulación global que establezca limitaciones legales tanto ex ante como ex post ante la utilización de mecanismos electrónicos de vigilancia masiva.

Este trabajo se ocupará de aquellos derechos que garantizan la Protección de Datos frente al poder del Estado, reconocidos en el texto de nuestra Constitución y en la Declaración Universal de los Derechos Humanos. El presente estudio revisa la evolución de las legislaciones relativas a la privacidad y la protección de datos en España en intima consonancia con Europa y la legislación comunitaria. Nos meteremos de lleno en las garantías constitucionales respecto al tema que nos trata, profundizando en los límites temporales y en los derechos de los mismos. Abordaremos la protección de datos en supuestos especiales, y concluiremos este estudio profundizando en las recomendaciones internacionales en dicha materia. Con objeto de lograr y ofrecer una mayor percepción de seguridad, hemos dotado nuestras ciudades de dispositivos capaces de monitorizar todas nuestras actuaciones, desde la esfera pública ya sea con fines de seguridad, persecución de los delitos o el control del tráfico, o desde el ámbito privado, mediante la vigilancia y control de zonas privadas, zonas residenciales o eventos desarrollados en locales o recintos abiertos al público. Esta suerte de videocontrol, genera, inquietudes y reflexiones que pueden colisionar con algunas garantías del estado de derecho.

Respecto a la adecuación legista de las nuevas tecnologías que se describirán en esta tesis tales como la video-grabación inteligente, la videograbación mediante drones, o la videograbación de manera continua a través de cámaras personales en los uniformes policiales, se está tomando en consideración por las autoridades, dedicándose importantes esfuerzos en investigación y desarrollo de nuevos y más eficientes métodos de video-grabación inteligente, hemos de concluir que la legislación española actual presenta dificultades para poder responder a la misma velocidad que la tecnología ofrece sus productos, y que incluso actualmente carece de reconocimiento en concreto, la legislación más pertinente, y que debería tener especial incidencia como la propia ley de enjuiciamiento criminal debiéndose

reiterar la necesidad de exigir al legislador, que se haga efectiva una urgente regulación completa de este medio adecuándose incluso contemplando los venideros sistemas de videovigilancia inteligente, con el objeto de no posibilitar vacíos legales que puedan originar inseguridad jurídica y, por consiguiente, ineficacia o la propia vulneración de derechos por un uso inadecuado de estos sistemas.

Si bien en España no se le ha prestado la importancia que en otros países ha supuesto la videovigilancia tales como Reino Unido o EEUU, la realidad en nuestro país nos muestra a través de las encuestas realizadas por el Centro de Investigaciones Sociológicas, durante los años 2008, 2009 y 2011, que en general se muestra un elevado nivel de apoyo al uso de cámaras, con cifras similares a las extraídas de encuestas de otros países citados, al incrementar la percepción de seguridad y protección ciudadana, y considerada por estos, como una medida eficaz en la lucha contra la delincuencia. Aunque este apoyo mayoritario se fragmenta cuando los dispositivos de vigilancia están situados en los lugares de trabajo (casi el 40% lo ven mal o muy mal), las comunidades de vecinos (rechazo de 27%) y las calles (25%).

La rápida adopción de dispositivos que nos mantienen permanentemente conectados y que llevamos en nuestros bolsillos y mochilas, así como la progresiva presencia de cada vez más dispositivos e interfaces incorporados en objetos y superficies capaces de procesar información digital representan un enorme cambio en nuestra experiencia vital y comportamientos habituales. La vida diaria se va colonizando de dispositivos que organizan o mediatizan nuestras decisiones principalmente mediante la extensión de los dispositivos móviles o incluso otros que toman decisiones por nosotros mismos de manera subrepticia y, en muchas ocasiones, independientemente de nuestra voluntad. Desde cámaras de reconocimiento facial en las esquinas de nuestras calles hasta farolas que detectan la presencia de personas en la acera, la realidad aumentada, o la dispositivos de control automático de las funciones de los servicios urbanos, hasta mecanismos que captan constantemente y registran nuestra posición etc.

Falta abordar entonces en este escenario y de una manera crítica el significado de este rastro digital y reconocer la necesidad de comprender con calma y de manera compleja el significado de este cambio tecnológico en la vida en la ciudad, un cambio profundo que sin una adecuada gestión podría provocar

rechazo social siendo necesario adaptar los sistemas para el cumplimiento de las leyes de protección de datos y de privacidad para proteger los derechos de los ciudadanos. La instalación de este tipo de sistemas de control hace que sea necesaria la protección de los derechos individuales de las personas observadas. La información procedente de las cámaras de seguridad, como puede aportar detalles sobre las personas y hacerla identificable, se trata como datos personales, y está regulada de forma general por diversos instrumentos jurídicos internacionales. Las transformaciones sociales y las distintas innovaciones tecnológicas han promovido la aparición de nuevos riesgos que colisionan con la esfera de distintos derechos de la esfera privada de la persona, tales como el derecho a la intimidad, derecho al honor y derecho a la imagen, en un marco en el que los daños ocasionados a estos bienes de la personalidad pueden resultar de muy difícil atribución y localización. La generalización en la actualidad de la videovigilancia de seguridad, como resultado del fenómeno y demanda por parte de la ciudadanía de mayores cotas de seguridad y a su vez, la tendencia y profusión de la era digital implementada a través de las denominadas Smart Cities, presentan igualmente un escenario donde los distintos derechos comprendidos en el art 18 CE, pueden verse doblegados. Generalmente, las lesiones a estos derechos se vinculaban en actividades profesionales en los que el supuesto infractor ejercitaba su libertad de expresión o información, resultando que en tales circunstancias, se mostraba con meridiana claridad cuál de los conflictos debía de prevalecer, dependiendo de una fundamentación adhoc, la consideración como ilegítima o no, la eventual intromisión y consecuentemente, la responsabilidad exigible al agente causante del daño. La posible vulneración de estos derechos cuando el agente causante se ampara en su derecho a la seguridad hace que no resulta tan fácilmente identificable cuál de los derechos prevalece. La delimitación del concepto y contenido de cada uno de estos derechos no resulta tarea sencilla. La doctrina advierte un tratamiento defectuoso, incurriendo banalmente a recursos tautológicos sobre el bien protegido, advirtiéndose como el legislador no brinda una definición o caracterización suficiente de la que puedan deducirse de forma exacta o definitiva el alcance, de los derechos de la esfera personal, motivado esta ambigüedad, por la directa relación de estos derechos en contextos históricos, sociales, culturales o jurídicos, en el que se encuadrasen, limitándose el legislador a otorgarles una mayor o menor protección en función de su carácter,

donde, en el caso de España, ha sido suplida si cabe, por parte del TS y el TC a la hora de acotar qué es lo que se protege con estos derechos. En este tesis observaremos la peculiaridad que subyace entre la colisión de los derechos a la esfera privada y el derecho a la seguridad a través de una reinterpretación del derecho a la seguridad como un súper derecho de la sociedad contemporánea actual, que se comprende en esta tesis, como un desplazamiento de la demanda social del Derecho penal como mecanismo de protección, sustituido por el auxilio estatal a través de una mayor intensidad de la actividad policial y los mecanismos de técnicos de los que esta dispone, tales como la videovigilancia. Este despliegue y énfasis del derecho a la seguridad, el legislador la fundamenta en aras de protección de la colectividad y del propio Estado, y la proyecta a través de la nueva Política criminal como instrumento de lucha contra el delincuente y el enemigo, observándose en esta tesis, un posible conflicto entre derechos. Las conductas de stalking, también denominado acecho o acoso predatorio, han hecho entrada en nuestro código penal. En este artículo, se realiza en primer lugar una definición del concepto y de sus características, centrándonos en particular a una de las manifestaciones del stalking, evolucionado como fenómeno actual y creciente, surgido a raíz de las nuevas tecnologías de la comunicación y de la información y que la doctrina denomina cyberstalking[1], observando en particular en este artículo, las consideraciones criminológicas sobre el perfil del acechador y a la víctima de la conducta de acoso o acecho a través de la red.

Por todo lo expuesto, veremos como a pesar de la expansión masiva de este tipo de programas todavía sabemos muy poco sobre su efectividad. La apuesta de los gobiernos por este tipo de intervención estaba basada en un puñado de estudios que presentaban en apariencia resultados positivos, pero que no empleaban grupos de control, se limitaban a observar diferencias entre el periodo anterior y el posterior a la implementación de la video-vigilancia, no siempre eran realizados con unos niveles apropiados de competencia profesional y, en general, eran evaluaciones realizadas por investigadores con vínculos al Home Office y,

[1] De acuerdo con Gregorie,M el cyberstalking es una extensión de la modalidad física de stalking., "Cyberstalking: Dangers on the Information Superhighway", National Center for Victims of Crime, 2001, pág.1. El término "cyberstalking" hace referencia al uso de Internet, ordenador o cualquier otra tecnología de la comunicación para acosar u hostigar a una persona. Como modalidad de stalking, se caracteriza por ser una conducta persistente y reiterada que causa un malestar a la víctima y afecta a su libertad de obrar.

por lo tanto, no eran evaluaciones independientes.

Welsh y Farrington (2002) realizaron una revisión sistemática de la literatura para el Home Office orientada a evaluar la efectividad de este tipo de intervenciones, así como, un metaanálisis de las mismas. Welsh y Farrington (2002) sólo incluyeron en esta revisión aquellos estudios que reunían un mínimo de criterios: la vídeovigilancia era el objeto de la intervención, se medían los niveles del delito antes y después de la intervención, el diseño tenía la suficiente calidad e incluía un área de control y un área experimental, el número de delitos en cada área antes de la intervención era al menos de 20. Esta revisión pudo encontrar 22 estudios que reunían estos criterios y que empleaban la vídeo-vigilancia en el centro de las ciudades o urbanizaciones de viviendas públicas, aparcamientos o transportes públicos. De los 22 estudios, la mitad encontraron que la delincuencia se había visto reducida como resultado de la vídeovigilancia, mientras que cinco estudios encontraron que la delincuencia había aumentado, otros cinco estudios no encontraron diferencias significativas y los resultados de un estudio aunque sugerían una reducción no eran del todo claros.

II

OBJETIVOS

II. OBJETIVOS

El objeto del presente Estudio de "Tesis Doctoral" dentro de la rama que la UCAM ofrece en Ciencias Sociales, tiene su fundamento en el tratar de profundizar en el tema relacionado.

1. Contextuar y conceptualizar los términos del derecho a la propia imagen, y el tratamiento de la imagen como dato personal
2. Definir la relación entre los derechos a la seguridad y los derechos de la esfera personal
3. Examinar los medios más efectivos y eficientes para disminuir la colisión de derechos de la "esfera íntima" en el desarrollo de la tecnologías de la imagen.
4. Analizar los factores de protección y riesgo de la videovigilancia
5. Analizar el objeto y finalidad de la videovigilancia y observar el rol de la videovigilancia como factor de victimización
6. Observar la legislación público-privada del tratamiento de la imagen y los nuevos retos que presentan dispositivos tipo Drone para la captura de imágenes.
7. Observar la pertinencia de las nuevas tecnologías de la videograbación policial
8. Describir los aspectos de la conducta humana ante el fenómeno de las Smart cities
9. Especificar propuestas al legislador sobre política criminal digital

III

METODOLOGÍA

III. METODOLOGÍA

Tal y como regula el artículo 34 de la Normativa de estudios oficiales de Doctorado, se establece la posibilidad de la Tesis por Compendio de Publicaciones. Por ello, la tesis doctoral consistirá en un trabajo original elaborado a partir del conjunto de publicaciones del doctorando relacionadas en el plan de investigación de la tesis doctoral.

A los efectos prevenidos en el párrafo anterior, el conjunto de publicaciones estará constituido por un mínimo de tres capítulos de libros, y un artículo de revista, relacionados con el objeto de la tesis, que serán publicados en editoriales de reconocido prestigio y que cuenten con sistemas de selección de originales por el método de evaluación externa o revisión ciega por pares.

La metodología empleada en el presente Estudio de "Tesis Doctoral" dentro de la rama que la UCAM ofrece en Ciencias Sociales, tiene su fundamento en la observación del tema relacionado con la colisión de derechos desde su perspectiva de regulación del derecho dentro de nuestro Ordenamiento Jurídico, así como desde la visión de la investigación dentro de entramado de la materia, para tratar de descubrir algunas conductas típicas que quedan impunes, la aplicación de las nuevas tecnologías, sobre todo en la vertiente dirigida a la adaptación normativa a las nuevas tecnologías.

Para poder llevar a cabo lo anteriormente expuesto, el estudio que vamos a realizar constituye un análisis cualitativo, ya que los análisis metodológicos empleados son: teóricos, manejando fuentes documentales y etnográficos, a través del análisis de realidades concretas.

Ante el planteamiento de llevar a cabo una investigación en la que se incluye el comportamiento humano y las normas sociales se piensa en términos de si la investigación ha de ser de tipo cualitativo o cuantitativo. En nuestro caso, el valor de las construcciones teóricas que incluye la investigación, conceptos, definiciones, representaciones, descripciones, etc, como hipótesis de perfectibilidad de una pequeña parte de la realidad social, dependen de la experiencia para su legitimación, y, a su vez, son el resultado de la coordinación de ideas recogidas en la experiencia, para aplicarlas a la mayor extensión posible.

Mediante la utilización de método fundamentalmente inductivo deductivo, basado en las fuentes de los diferentes ordenamientos, así como de los estudios doctrinales existentes sobre la materia, realizaremos un exhaustivo análisis sustantivo de los documentos encontrados.

Dentro de las técnicas metodológicas que hemos utilizado, destaca la observación documental a través de:

- Metaanálisis: búsqueda documental y tratamiento de datos
- El análisis de contenidos: unidades de análisis, categorización, codificación y cuantificación
- El análisis secundario: fuentes de datos, análisis e interpretación

La documentación analizada incluye monografías, revistas especializadas, nacionales e internacionales, fuentes demográficas e históricas, prensa y conferencias. Todo ello para aportar rigor científico a la presente obra.

.

ESTADO DE LA CUESTIÓN

IV. ESTADO DE LA CUESTIÓN

Este trabajo se ocupará de aquellos derechos que garantizan la Protección de Datos frente al poder del Estado, reconocidos en el texto de nuestra Constitución y en la Declaración Universal de los Derechos Humanos. El presente estudio revisa la evolución de las legislaciones relativas a la privacidad y la protección de datos en España en intima consonancia con Europa y la legislación comunitaria. Nos meteremos de lleno en las garantías constitucionales respecto al tema que nos trata, profundizando en los límites temporales y en los derechos de los mismos. Abordaremos la protección de datos en supuestos especiales, y concluiremos este estudio profundizando en las recomendaciones internacionales en dicha materia.

El Derecho a la Protección de Datos y el ejercicio de las libertades públicas constituyen un binomio inseparable, y ambos conceptos son requisitos básicos de la convivencia en una sociedad democrática. Una de las conquistas más importantes de la sociedad, en su búsqueda de hitos fundamentales para regular la convivencia tanto a nivel nacional como internacional, ha sido, sin duda, el consenso alcanzado respecto a la noción de Derechos Humanos y plasmada en la Declaración Universal de 1948[2]. Pero no es menos cierto que, junto a solemnes y amplios textos internacionales que los reconocen, la historia ha conocido y aún conoce brutales violaciones e incumplimientos de los mismos. Es por ello, la importancia de establecer mecanismos jurídicos idóneos para garantizarlos, a través de un proceso denominado: positivación de los derechos humanos.

LA DIRECTIVA 95/46/CE[3]

En 1981 se aprobó el, ya comentado, Convenio nº 108 del Consejo, sobre la protección de las personas en lo relativo al tratamiento automatizado de datos de

[2] El 10 de diciembre de 1948, la Asamblea General de las Naciones Unidas aprobó y proclamó la Declaración Universal de Derechos Humanos. Tras este acto histórico, la Asamblea pidió a todos los Países Miembros que publicaran el texto de la Declaración y dispusieran que fuera "distribuido, expuesto, leído y comentado en las escuelas y otros establecimientos de enseñanza, sin distinción fundada en la condición política de los países o de los territorios".

[3] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31. Se puede consultar en http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm

carácter personal, primera norma europea que marcó las pautas del modelo común de protección de datos[4]. Se establecen una serie de principios básicos para la protección de datos, señala criterios que regulan su flujo y crean una Comisión, a quien se encomienda la formulación de propuestas para mejorar la aplicación del Convenio.

El 18 de julio de 1990 la Comisión presenta al Consejo, la primera propuesta de Directiva, junto con la propuesta sobre tratamiento de los datos personales y protección de la vida privada en el sector de las telecomunicaciones[5], que fue sustituida, debido a los avances técnicos que con el paso del tiempo se fueron produciendo, por la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, ampliando su cobertura al tratamiento de los datos personales y a la protección a la intimidad en el ámbito de las comunicaciones electrónicas[6]. Con posterioridad y para modificar ciertos aspectos de esta última se presenta una nueva Directiva sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[7].

La Directiva 95/46/CE se aprueba el 24 de Octubre de 1995[8] con la voluntad de acercar las legislaciones estatales de protección de datos personales sentando las bases para lograr la coordinación de las legislaciones nacionales aplicables en aras a garantizar la libre circulación de tales datos entre los Estados Miembros.[9]

En la sociedad y a lo largo de los años, se ha ido formando la "*conciencia*

[4] El Convenio pretendía ampliar la protección de los derechos y las libertades fundamentales y, en concreto, el derecho al respeto a la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos informatizados. Puede consultarse el estado de adhesiones al convenio en el siguiente enlace: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG

[5] Directiva 97/66/CE, de 15 de diciembre de 1997, DO L 24 de 30.1.1998.

[6] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002.

[7] Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de Marzo de 2006.

[8] BOE. Nº 181, de 30 de Junio de 1991.

[9] Considerando n.º 7 de la directiva 95/46/CE: "Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros".

europea sobre protección de datos"[10]. Uno de los frutos de esta conciencia ha sido la Directiva 95/46/CE de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta a los datos personales y a la libre circulación de éstos, surgida con la firme intención de ampliar y puntualizar lo relativo a la protección de datos, dada la disparidad legislativa de los Estados miembros así como el desfase y la generalidad del Convenio 108. Se atiende así a la necesidad de una normativa más concreta y definida, un fondo común en cuanto a la protección de datos y la preservación de los derechos fundamentales con un ámbito europeo.

La Directiva establece como eje central de su contenido el derecho a la intimidad[11], sin que ello excluya la entrada en juego de otros intereses estatales para proteger la información más allá de la frontera europea, o en su caso, impedir la salida de datos del territorio comunitario. Por una parte son motivos de seguridad pública, defensa y seguridad del Estado, y también el que los datos representan una cultura, un patrimonio que es propio de los Estados. Se inscribe, como lo ha señalado la propia Comisión, en el contexto de la creación de un espacio europeo de información en el que el tratamiento de datos personales aumentará de forma sustancial[12]

En lo referente al ámbito de aplicación, establece que los principios incluidos en su contenido serán de aplicación a todos los tratamientos de datos personales en los que el responsable del fichero o responsable del tratamiento[13] se encuentre

[10] DAVARA RODRÍGUEZ, M. A. La protección de datos personales en el sector de las telecomunicaciones, cit., pp. 8-10.

[11] Considerando n.º 7 de la directiva 95/46/CE: "Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales."

[12] CONDE ORTIZ, C. Análisis de la legislación en el ámbito comunitario sobre el derecho a la protección de datos de carácter personal, cit.,pp.55

[13] El concepto "responsable del tratamiento" se introduce en el Convenio 108 del Consejo de Europa, "significará la persona física o jurídica, autoridad pública, servicio u otro organismo que según la ley nacional fuere competente para decidir sobre qué clases de datos de carácter personal deben ser almacenados y qué operaciones deberán serles aplicadas". El concepto aparece más restringido en la Directiva por cuanto que el responsable lo será con sólo decidir sobre los fines y los medios del tratamiento. La propia Directiva establece que "cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerado normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales

dentro del ámbito de aplicación del Derecho Comunitario.

Asimismo, considera la Directiva 95/46/CE que su ámbito de aplicación recae exclusivamente sobre las personas físicas[14], que habríamos de entender se refiere a una remisión al Convenio 108. El Derecho comparado no ofrece una solución unitaria a esta cuestión, ya que mientras unos países excluyen a las personas jurídicas, otros han optado por incluirlas como titulares del derecho. Entre los países que excluyen a las personas jurídicas, se encuentran Alemania, España, Francia, Irlanda, Países Bajos, Portugal, Reino Unido y Suecia. Entre los que las incluyen están Austria, Dinamarca, Islandia, Luxemburgo y Noruega[15].

Los aspectos a considerar más destacables contemplados por la Directiva son:

- Se establecen medidas aplicables tanto para ficheros automatizados como para ficheros manuales[16]. Las disposiciones se aplicarán al tratamiento total o parcialmente automatizado de datos personales, quedando excluido el tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas y en cualquier caso cuando el tratamiento tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.
- Se amplia el concepto de dato de carácter personal incluyendo dentro del mismo la imagen y el sonido[17], dedicando a estos datos personales 4 de sus

complementarios y necesarios para el funcionamiento del servicio".

[14] Considerando nº 24 de la directiva 95/46/CE: "que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que le conciernen no son objeto de la presente Directiva".

[15] LUCAS MURILLO DE LA CUEVA, P.: Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal). Centro de Estudios Constitucionales. 1993. pag. 50.

[16] Directiva 95/46/CE, Capitulo I, Art. 3 Ámbito de aplicación.

[17] Considerando n.º 14 de la directiva 95/46/CE: "que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;"

Considerando n.º 15 de la directiva 95/46/CE: "que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;"

Considerando n.º 16 de la directiva 95/46/CE: "que los tratamientos de datos constituidos por sonido

72 considerandos.

- Se contempla la posibilidad de solicitar el ejercicio de un nuevo derecho como es el Derecho de Oposición[18]. Con ello se da derecho al interesado a oponerse en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa, y a oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.
- La posibilidad de conciliar el derecho a la intimidad con la libertad de expresión, estipulando que en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión[19].
- Se incluyen los datos sindicales dentro de categorías especiales de datos[20], precisando que los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Haciendo la

---

e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario"

Considerando n.º 17 de la directiva 95/46/CE: "que en lo que respecta al tratamiento del sonido y de la imagen aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, los principios de la Directiva se aplican de forma restringida según lo dispuesto en al art.9".

[18] Directiva 95/46/CE. Cap. II, sección VII. Artículo 14. Derecho De Oposición Del Interesado.

[19] Directiva 95/46/CE. Cap. II, sección III. Artículo 9. Tratamiento de datos personales y libertad de expresión

[20] Directiva 95/46/CE. Cap. II, sección III. Artículo 8. Categorías Especiales De Tratamientos.

salvedad cuando el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados.

- Se crea una nueva figura, el encargado del tratamiento. El concepto de «responsable del tratamiento», antes citado, y su interacción con el concepto de "encargado del tratamiento[21]" desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos, cómo pueden ejercer sus derechos los interesados, cuál es la legislación nacional aplicable y con qué eficacia pueden operar las autoridades de protección de datos, dejando asimismo contemplado en la directiva el termino "tercero[22]", en consonancia con los anteriores.

En lo referente a la calidad de los datos, establece la Directiva cinco principios esenciales: los datos han de ser tratados de manera leal y lícita; los fines a que obedece la recogida de datos habrán de ser determinados, explícitos y legítimos; los datos han de ser adecuados, pertinentes y no excesivos; los datos habrán de ser exactos y actualizados; y asimismo deberán ser conservados en una forma que permita la identificación de los interesados[23].

A destacar en el Art. 7 de la Directiva, los *Principios relativos a la Legitimación del tratamiento de datos[24];* los Estados miembros dispondrán que el tratamiento de datos personales sólo podrá efectuarse si:

---

[21] Directiva 95/46/CE. Cap. I, Artículo 2. Definiciones "e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;".

[22] Directiva 95/46/CE. Cap. I, Artículo 2. Definiciones "f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;".

[23] Directiva 95/46/CE. Cap. II, Sección I, Artículo 6, Principios Relativos a la Calidad de los Datos.

[24] Directiva 95/46/CE. Cap. II, Sección II, Artículo 7, Principios relativos a la Legitimación del tratamiento de datos.

- El interesado presta su consentimiento de forma inequívoca.
- Es necesario para la ejecución de un contrato en el que el interesado sea parte.
- Fuese necesario para el cumplimiento de una obligación jurídica a la que éste sujeto el responsable del tratamiento.
- Es necesario, para proteger el interés vital del interesado.
- Es en misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento, o de un tercero a quien se comuniquen los datos.
- Es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

Encontramos sin duda la motivación legislativa de esta Directiva, en los setenta y dos considerandos[25] que presenta, y de los que merecen mención:

- El tratamiento lícito, cuando se efectúa con el fin de proteger un interés esencial para la vida[26].
- El eje vertebral de la protección de datos, el consentimiento. Los datos que por su naturaleza puedan atender contra las libertades fundamentales o intimidad, únicamente pueden ser tratados si existe el consentimiento explícito del interesado. Además muestra que deberá informarse al interesado en el momento del registro de los datos, o a más tardar, al comunicarse los datos por primera vez a un tercero[27].

---

[25] REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española, 22ª edición. Considerando. (Ger. de *considerar*). 1. m. Cada una de las razones esenciales que preceden y sirven de apoyo a un fallo o dictamen y empiezan con dicha palabra.''

[26] Considerando n.º 31 de la directiva 95/46/CE: ''Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado''.

[27] Considerando n.º 30 de la directiva 95/46/CE: ''Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a

- La finalidad. Será tratamiento leal aquél en el que el interesado conozca la existencia del tratamiento y que se le informe en la recogida del dato de manera precisa y completa de cual será su tratamiento y utilización[28].
- El derecho de acceso. Método de comprobación de la exactitud y licitud del tratamiento, así como la posibilidad de conocer el sistema lógico que subyace al tratamiento automatizado[29].
- Y la seguridad. Obligando a garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse[30].

---

terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan;"

Considerando n.º 33 de la directiva 95/46/CE: "Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales".

[28] Considerando n.º 38 de la directiva 95/46/CE: "Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención".

[29] Considerando n.º 41 de la directiva 95/46/CE: "Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informático; que no obstante esto no debe suponer que se deniegue cualquier información al interesado".

[30] Considerando n.º 46 de la directiva 95/46/CE: "Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el

En lo relativo a la *Transferencia de datos personales a países terceros*, menciona la Directiva que la cesión ha de ser acorde con el derecho nacional y únicamente podrá realizarse en el caso, de que el país que recibe los datos, tenga un nivel de garantía de los mismos adecuado y que la adecuación se medirá en base a lo equiparable que esté la protección de datos con la regulación europea a lo que suma una larga enumeración de excepciones.

La Directiva 95/46/CE fundamenta la licitud de las transferencias en el concepto de "nivel de protección adecuado", que a juicio de Heredero Higueras[31], constituye una exigencia más débil que el nivel de protección requerido en el Convenio 108 del Consejo de Europa. Bien es verdad que en el ámbito comunitario, y visto el ámbito de aplicación a que se refiere la Directiva, intentar adoptar el concepto "nivel de protección equivalente" presentaba importantes dificultades, tanto en el ámbito práctico como en el legislativo, por cuanto que se significaría la necesidad de determinar en el ámbito comunitario pero con extensión al resto del mundo un principio general a nivel mundial para dichas transferencias –entre Estados miembros y terceros- lo cual no puede ser factible. Por otra parte, el fundamento y la significación de las transferencias de datos en el texto definitivo adquiere una nueva orientación, fundamentalmente porque la transferencia deja de ser ilícita por principio en el caso de que en el Estado de destino exista un nivel de protección adecuado o en el de que no exista tal nivel cuando se den las condiciones de licitud o unas garantías especiales principalmente contractuales[32].

En general, acerca de la transferencia internacional de datos son alarmantes las numerosas excepciones y la indefinición jurídica de muchos de los conceptos utilizados[33]. En nuestro país, la transición de la normativa se hizo fuera de plazo ya que éste finalizaba el 25 de Octubre de 1998.

TRANSPOSICIÓN DE LA DIRECTIVA 95/46/CE A LA LEGISLACIÓN ESPAÑOLA EN PROTECCIÓN DE DATOS.

La Ley orgánica 15/1999, de Protección de Datos de Carácter Personal, de 13

tratamiento y con la naturaleza de los datos que deban protegerse".

[31] HEREDERO HIGUERAS, M. La Directiva Comunitaria de Protección de los Datos de Carácter Personal. Edit. Aranzadi. 1996

[32] HERRÁN ORTIZ, A. I. La directiva 95/46/CE de protección de las personas frente al tratamiento de sus datos personales y de la libre circulación de estos datos. Vid: http://libros-revistas-derecho.vlex.es/vid/directiva-frente-libre-circulacion-190765

[33] Así lo entiende REBOLLO DELGADO, L. y SERRANO PÉREZ, M. M. *Introducción a la Protección de Datos*, op. cit., p. 42.

de diciembre, (LOPD), norma que viene a transponer a la legislación española la Directiva 95/46/CE, y que deroga a la precedente Ley orgánica reguladora del Tratamiento Automatizado de Datos de Carácter personal, de 1992.

La Ley, que nace con una amplia vocación de generalidad, prevé en cuanto al objeto, garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar[34].

Sin embargo, pese a la teórica sencillez y claridad que emana de esta norma en relación al objeto protegido por la misma, nos encontramos, por el contrario, ante verdaderas dificultades a la hora de definir de manera pormenorizada cuál es el objeto al que se refiere. Estas dificultades han tenido su reflejo en un extenso debate doctrinal, que vino a apaciguar en gran medida el Tribunal Constitucional en el año 2000 a través de la sentencia 292/2000 de 30 de noviembre[35], en la que el objeto de protección del derecho fundamental a la protección de datos, nos dice el Tribunal Constitucional, no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que ya estaría protegido por el artículo 18.1 de la Constitución, sino los datos de carácter personal.

El Tribunal Constitucional, por medio de esta Sentencia, viene a establecer el derecho a la protección de datos como derecho fundamental autónomo, siendo, por ende, merecedor de la más elevada protección por parte de nuestro ordenamiento jurídico y cuyo contenido está integrado por los principios y derechos que se contemplan en la Ley Orgánica 15/1999. En virtud de este derecho fundamental, el ciudadano, con carácter general, puede decidir sobre sus propios datos.[36]

Asimismo, la reciente Sentencia del Tribunal Supremo de fecha 8 de Febrero de 2012[37] es otra muestra de la incongruente transposición en España de la

[34] Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, Título I, Art. 1
[35] YANGUAS GÓMEZ, R. El Tratamiento Invisible de Datos de Carácter Personal en Internet. REDUR nº 2 / Año 2004.
[36] SUERO SALAMANCA, J. A. Comentarios a la Sentencia del T. C. 292/2000, de 30 de Noviembre. Vid: http://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf
[37] STS (Sala 3) de 8 de febrero de 2012. Protección de datos de carácter personal. Principio del consentimiento. Nulidad del artículo 10.2.b) del Reglamento de la LOPD

Directiva 95/46/CE en la medida que, mientras la Directiva parte de definir una serie de supuestos para el tratamiento, la Ley Orgánica 15/1999 de Protección de Datos opta por legitimar el tratamiento o la cesión de datos sobre la base del consentimiento inequívoco del interesado y, a partir de esa figura, sentar una serie de excepciones. Por su parte, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal en su artículo 10, estableció una serie de bases para que se pudieran desarrollar alguna de las excepciones marcadas en la Ley Orgánica[38].

LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Como bien hemos ido apuntando, la protección de datos es una defensa de los derechos fundamentales del individuo proclamados en la Constitución Española de 1978, como el derecho de intimidad personal de nuestro Art.18.4: "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". Por tanto, su fundamento radica en proteger la dignidad de la persona, constituir un ámbito de libertad del individuo y una concreción inapelable de los derechos clásicos de la personalidad, como son el honor, la intimidad y la propia imagen.

Los derechos del artículo 18 CE al encontrarse en la Sección 1ª del Capítulo II del Título I de la Constitución están sometidos a reserva de ley orgánica (art. 81 CE), que en todo caso deberá respetar su contenido esencial, y vinculan a todos los poderes públicos (art. 53.1 CE), y, entre las garantías jurisdiccionales podrá recabarse la tutela de los tribunales ordinarios mediante un procedimiento basado en los principios de preferencia y sumariedad y, subsidiariamente, la tutela del Tribunal Constitucional mediante un recurso de amparo (art. 53.2 CE)[39].

La protección de los datos frente al uso de la informática es nuestra Constitución una de las primeras en introducirlo dado que es precisamente en los años de su redacción cuando comienzan a apreciarse los peligros que puede entrañar el archivo y uso ilimitado de los datos informáticos. En este sentido, la

[38] Así lo explica: ALONSO MARTÍNEZ, C. "*La armonización de la normativa de protección de datos a las normas comunitarias"* Artículo publicado a 5 de Marzo de 2012. Diariojuridico.com

[39] ELVIRA PERALES, A. *Sinopsis artículo 16 Constitución Española*. Vid: http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=16&tipo=2

Ley no parte de una perspectiva negativa respecto a las nuevas tecnologías. La informática, mecanismo esencial del progreso social, no debe ser limitada, sino que ha de adaptarse con la necesaria indemnidad y protección de los derechos fundamentales.

La idea en un primer momento era presentar la reforma de la LORTAD sin la redacción de una nueva ley, pero el elevado número de enmiendas provocó la existencia de una nueva norma. La LOPD que entró en vigor el 14 de Enero del año 2000, que consta de siete títulos, cuarenta y nueve artículos, seis disposiciones adicionales, tres disposiciones transitorias, una derogatoria y tres disposiciones finales, con el delusorio aspecto en relación a su precedente de no disponer de una exposición de motivos.

En cuanto al ámbito de aplicación, dispone que afectará tanto al territorio español como al marco internacional, aplicando las normas de Derecho Internacional Público, aún cuando el responsable no esté establecido en territorio español pero haga uso para el tratamiento de datos medios o en transito situados en territorio español[40].

El Título III de la Ley, referente a los *Derechos de las Personas*, que aunque ya se incluían en la LORTAD, se recoge la aportación de la DIRECTIVA 95/46/CE, el derecho de oposición. Es de tenacidad concebir que estos derechos que se otorgan son el concluyente de esta Ley, sino el segundo eje vertebral, tras el citado consentimiento. Y con respecto a la concreción y ampliación de los derechos de los titulares de los datos, nos aporta la Ley:

- Derecho a no soportar valoraciones automáticas[41], "Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos

[40] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo I, Artículo *2*. Ámbito de aplicación. "1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a. Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b. Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c. Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito."

[41] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo III, Artículo 13. Impugnación de valoraciones.

o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.". "El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad".

- Derecho de consulta al Registro General de Protección de Datos. Este derecho implica la consulta pública y gratuita para cualquier interesado del Registro en el cual se inscriben las características esenciales del tratamiento[42].
- Derecho de Acceso en su Art. 15 "El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos".
- Derecho de rectificación y cancelación[43]. La cancelación dará lugar al bloqueo de los datos, y la rectificación obliga al Responsable del Fichero a atender cualquier solicitud de modificación sobre los datos de carácter personal del interesado.
- Derechos de oposición. Dos preceptos de la Ley acogen este derecho, el Art. 6.4 "En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal". En cuanto a los ficheros destinados a la publicidad y/o prospección comercial directa, se prescribe que "los interesados tendrán derecho a oponerse, previa petición y sin gastos al tratamiento de los datos que los conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud" y el Art. 30.4, alusivo a los tratamientos de datos con fines de prospección comercial y publicidad directa fija que "los interesados tendrán derecho a oponerse, previa petición y sin gastos al tratamiento de los datos que le conciernan, en cuyo caso serán dados

[42] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo III, Artículo 14. Derecho de consulta al Registro General de Protección de Datos.
[43] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo III, Artículo 16. Derecho de rectificación y cancelación.

de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud."

- Derecho a indemnización[44]. Los interesados que sufran daños como consecuencia del incumplimiento de lo dispuesto en la Ley, por el responsable o encargado del tratamiento, tienen derecho a ser indemnizados.

Importancia ofrece en el texto de la Ley analizado, la obligación de revelar las medidas de seguridad existentes en ficheros de titularidad pública, para proceder a la creación, modificación o supresión de dichos ficheros; se establecen además las exigencias de cumplimiento para los ficheros de las empresas que realizan actividades de prestación de servicios de información sobre solvencia patrimonial y crédito.

Se incide en la necesidad de autorización de *transferencia internacional de datos* por parte de la Agencia de Protección de Datos y los requisitos que considera la misma para realizarlas a países con niveles distintos de seguridad a España, y por otro lado, aumenta los supuestos en los que no requiere dicha autorización.

Como hemos visto, el principio general que consagra la Directiva 95/46/CE y que ahora encontramos en la LOPD es la prohibición de realizar transferencias temporales o definitivas de datos con destino a países que no proporcionen un nivel de protección equiparable al de la Unión Europea.

La LOPD paralelamente a lo dispuesto en la Directiva, consagra el principio general de la "permisividad de la transferencia" en aquellos supuestos en los que el país de destino proporcione un nivel equiparable al de la LOPD en lo referido a la protección salvo que "además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, qué sólo podrá otorgarla si se obtienen garantías adecuadas[45]".

La exigencia de la obtención de autorización de la Agencia de Protección de Datos se exime en la LOPD con un amplio listado de excepciones recogidas en su Titulo V, Art. 34.

Tal es la relevancia que hoy por hoy ha adquirido este tipo de movimientos internacionales de datos, en particular en el ámbito empresarial, dadas las nuevas

[44] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo III, Artículo 19. Derecho a indemnización.
[45] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo VI, Movimiento Internacional de Datos. Artículo 33.1. Norma general.

tecnologías y el surgimiento del Cloud Computing[46] que además de lo encomendado en la LOPD la Agencia Española de Protección de Datos, desarrolla en Diciembre de 2000 una Instrucción especifica en esta materia[47].

Respecto al *Régimen Sancionador* aplicable descrito en el Titulo VII de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* ha sido recientemente modificado en base a la disposición final quincuagésimo octava de la Ley de Economía Sostenible[48], que constituye una mejora y atemperación del régimen sancionador existente.

Exceptuando lo establecido para la Prescripción en el Art. 47 del Título VII de la LOPD, las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año y lo relativo al procedimiento sancionador y la potestad de inmovilización de ficheros en los Art. 48[49], la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal queda modificado"[50].

Atiende además esta reforma a lo solicitado desde algunos sectores; Alonso Hernández, especialista en Sistemas de Información, señala que: "encontramos, por otro lado, positiva la inclusión de más supuestos a tener en cuenta en la graduación de las infracciones. Entre ellos se encuentra, el volumen de negocio o actividad del infractor, por lo que parece que se está refiriendo a si se trata de una gran empresa o una pyme. Este criterio corrector está en la línea defendida desde

---

[46] RUBÍ, J. y BLANCO, M. J. Cloud Computing: sujetos que intervienen, ley aplicable, garantías. Transferencias Internacionales de Datos. 4ª Sesión Anual Abierta de la AEPD.

[47] Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos.

[48] Ley 2/2011, de 4 de marzo, de Economía Sostenible. Vid: http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-20iones 11-4117.pdf

[49] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Titulo VII, Infracciones y Sanciones**:**

"Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título. 2. Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa. 3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses."

[50] *Ley 2/2011, de 4 de marzo, de Economía Sostenible.* Disposición Final Quincuagésima Sexta. Modificación de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal

el Consejo General de Colegios de Economistas desde hace años y transmitida a la Agencia de Protección de Datos, a favor de una específica regulación o consideración de protección de datos para las pymes, así como en la consulta remitida recientemente desde RASI-CGCEE a la Comisión Europea, que por fin el legislador parece tener en consideración"[51].

En base a esto, la cuantía de las sanciones se gradúa según este nuevo régimen, bajo la observancia de criterios como el carácter continuado o reincidente de la infracción, el volumen de negocio o actividad del infractor en consonancia con los beneficios obtenidos como consecuencia de la comisión de la infracción, así como el grado de intencionalidad, los perjuicios causados a las personas interesadas o a terceras personas y cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad en la actuación infractora.

Asimismo, y en referencia a la potestad de inmovilización de ficheros también se apuntan las siguientes estipulaciones:

"En los supuestos constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y en particular de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas."

Como elementos destacables, figura la reducción de la cuantía económica en las sanciones impuestas a infracciones leves, la fijación de criterios objetivos estableciendo mayor concreción de los tipos infractores, la inclusión de un mayor número de parámetros para la ponderación y graduación de las sanciones, así

[51] Publicación del Registro de Economistas Auditores de Sistemas de Información, RASI, órgano especializado del Consejo General de Colegios de Economistas, "*Economistas señalan que La reforma de la Ley de Protección de Datos podría iniciar un cambio en el tratamiento de las PYMES*" Vid: http://static.diariojuridico.com/wp-content/uploads//kalins-pdf/singles/economistas-senalan-que-la-reforma-de-la-ley-de-proteccion-de-datos-podria-iniciar-un-cambio-en-el-tratamiento-de-las-pymes.pdf

como la ordenación de criterios para la aplicación de grado inferior y, por último, la aportación de la figura del apercibimiento al infractor, con carácter excepcional[52].

Su precedente: la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

La preocupación por la protección de datos de carácter personal en consonancia con los avances de la técnica y la informática, e intentando dar cumplimiento al ya mencionado Art. 18.4 de la Constitución Española y el compromiso adquirido en el Convenio 108, generó la creación de un Anteproyecto de ley en el año 1984 que nunca saldría a la luz como Ley, pero que si supuso fundamentos a incluir en otras normas, relativas a distintas materias persiguiendo la protección en el tratamiento de datos y el respeto a la intimidad del individuo.

Tras encontrarse varios años detenida la cuestión de manos de los Legisladores, España firma adhesión al Convenio de Schengen, con lo que nos obligamos a desarrollar la normativa necesaria que garantice el nivel de protección de los datos de carácter personal contemplados en el Convenio 108.

Es referencia obligada, hablar de la exposición de motivos que incluye esta Ley, en los que define el espíritu seguido por el legislador, haciendo mención al ámbito de aplicación que tendría la Ley y analizando con detalle el concepto de intimidad. La LORTAD, tiene como objeto principal la regulación de ficheros automatizados, olvidando los ficheros manuales o en soporte papel, que en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (LOPD) ya están regulados.

Fue una Ley muy criticada por la diferencia en el tratamiento que se realizaba con los datos de carácter personal utilizados para el ámbito privado, al tratamiento de los ficheros de titularidad pública, con innumerables excepciones que producían una, prácticamente, nula efectividad de protección de derechos. Ello conllevó a la presentación de consecutivos recursos al Tribunal Constitucional por el Defensor del Pueblo y el Partido Popular. Igualmente el Consejo ejecutivo de la Generalitat de Cataluña presentó un recurso ante el Tribunal Constitucional al considerar que esta norma no respetaba el marco de distribución de las

[52] GARCÍA, A. Directora Jurídica del Grupo Antevenio. Articulo publicado en Diario Jurídico. Vid: http://www.diariojuridico.com/opinion/la-modificacion-del-regimen-sancionador-de-la-lopdC2%BFsatisface-expectativas.html

competencias entre el Estado y las Comunidades Autónomas.

El Tribunal Constitucional resolvió las divagaciones con la Sentencia del 290/2000 de 30 de Noviembre[53] en la que se declara la pérdida sobrevenida de los recursos interpuestos por el Partido Popular y el Defensor del Pueblo y la desestimación del presentado por la Generalitat.

Determinados puntos incluidos en la LORTAD, son constituyentes de normativa vigente en la actualidad, como se establece en la disposición tercera de la LOPD. Asimismo, en el tiempo de vida de la LORTAD, la Agencia Española de protección de Datos elaboró necesarias Instrucciones[54] en materias que al no tener carácter reglamentario, no sientan normativa en vigor, por lo que resulta bastante impugnable su aplicación, aunque se puede comprobar como actualmente dicho Ente las aplica a nivel interpretativo. El motivo de la redacción de una nueva norma y derogación de la LORTAD, fue la necesidad de adaptación española a la Directiva 95/46/CE.

LA TRANSICIÓN DEL RD 994/1999: REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS AL RD 1720/2007, REGLAMENTO DE DESARROLLO DE LA LOPD.

El tardío nacimiento del derogado Real Decreto 994/1999[55], de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, surge como imprescindible desarrollo reglamentario de la derogada LORTAD[56], que preveía en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos

[53] Sentencia 290/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recursos de inconstitucionalidad contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal. Vid: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/Sentencia2901.PDF

[54] Los citados textos:- Instrucción 1/1995, Instrucción 2/1995, Instrucción 1/1996, Instrucción 2/1996 y la Instrucción 1/1998 de la AEPD.

[55] Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Vid: http://www.boe.es/boe/dias/1999/06/25/pdfs/A24241-24245.pdf

[56] La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal

almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Así la seguridad se configura no solo como un principio de la protección de datos, sino como un condicionante previo al tratamiento de los mismos, el cual además también ha sido objeto de preocupación por Legislador europeo quien, en la Directiva comunitaria[57] relativa al tratamiento de los datos de las personas establece en su Considerando 25 que, los principios de la protección tienen su expresión en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos-obligaciones, en particular, entre las que se incluye la seguridad técnica[58].

Con la posterior aprobación de la LOPD y a fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprobó el estatuto de la Agencia Española de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollaron determinados aspectos de la LORTAD y el texto que nos ocupa, Real Decreto 994/1999, de 11 de junio, por el que se aprobó el reglamento de medidas de seguridad de los ficheros automatizados que contuvieran datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la LOPD.

El motivo de la derogación del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal por la llegada del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de

[57] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos.

[58] MARZO PORTERA, A., coordinada por ALMUZARA ALMAIDA, C. en *Estudio Práctico sobre la protección de Datos de Carácter Personal*,2ª Edición, op. cit., p. 595-597

datos de carácter personal se dio fundamentalmente porque su anterior databa de 1999, y llegado el momento se había adquirido mucha experiencia nueva. Contemplando la transición de estos textos podemos comprobar que se pasa de 29 a 158 artículos.

La evolución más notable en la transición del antiguo reglamento al actual, es la contemplación de medidas de seguridad para ficheros en papel y la circunspección de los ficheros manuales (no automatizados) o mixtos (parte automatizada y no automatizada) dentro de la regulación otorgando a los interesados la plenitud de sus derechos respecto a lo contemplados en la Ley 15/1999**.**

El RD 994/1999, anterior a la aprobación de la LOPD de 13 de Diciembre de ese mismo año, no regulaba en ninguno de sus artículos los ficheros en papel, sólo los automatizados, dado que este se encontraba redactado en base a lo dispuesto por la precedente, la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

De las novedades que la necesidad había puesto de manifiesto, dentro de la experiencia que al legislador le otorga el tiempo transcurrido desde la aprobación del anterior reglamento, existían ciertos aspectos, no contemplados y que quedan aclarados en el RD 1720/2007, como por ejemplo con la exclusión de los ficheros realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas[59] y además supone en ciertas carencia de la LOPD su reglamento de desarrollo, mientras que el RD 994/1999 se centraba únicamente en las medidas de seguridad aplicables a ficheros automatizados.

Si la positiva evolución de la LORTAD a la LOPD supuso un aprendizaje de

[59] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
Título I, artículo 4. Ficheros o tratamientos excluidos: **"**El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:
a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.
b) A los sometidos a la normativa sobre protección de materias clasificadas.
c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos."

los legisladores para con la realidad de preservar el derecho fundamental a la protección de datos, en mi humilde opinión, la evolución que coexistió a la aprobación del Reglamento 1720/2007 supuso un paso de gigante en lo referido al cumplimiento de la protección de datos para los sujetos obligados, y una apertura de lindes a los derechos de los interesados y afectados.

Uno de los logros del nuevo Reglamento de desarrollo de la LOPD (RDLOPD)[60] radica en resolver las dudas interpretativas existentes en torno en la aplicación de la citada norma. Inciden los cambios en los siguientes aspectos:

Obtención del consentimiento y deber de información. Con relación a la exigencia de obtener el consentimiento del afectado o interesado, consigue especial atención el hecho de que el nuevo Reglamento incluye dos nuevas excepciones: cuando el tratamiento o cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o cesionario, o cuando sean necesarios para el cumplimiento de un deber jurídico.

*Tratamiento de datos de menores de edad***.** Se permite el tratamiento de los datos con el consentimiento de los padres o tutores sin excepción alguna.

Encargados del tratamiento y cesión de datos. Como contenido a reseñar, se determina que, aquel que accede a los datos con ocasión de la prestación de un servicio solicitado por el responsable, se consideraría que ha existido comunicación de datos cuando dicho acceso tenga por objeto el establecimiento de un nuevo vínculo entre el encargado del tratamiento y el interesado. Además se recoge expresamente la necesidad de obtención de autorización para la subcontratación por parte del Encargado del tratamiento y no se puede obviar que se traslada al responsable del fichero la obligación de velar por que el encargado reúna las garantías para el cumplimiento de la normativa de protección de datos de carácter personal[61].

Derechos de los titulares de los datos. En el Título III del RDLOPD, destinado a los Derechos de acceso, rectificación, cancelación y oposición y que se prolonga dese el Art. 23 hasta el Art. 36, se estipula que a fin de garantizar el ejercicio de los

[60] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
[61] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Capítulo III, Encargado del tratamiento. art. 20, 21 y 22.

derechos de acceso, rectificación, cancelación y oposición, el Reglamento dispone que deberá concederse al afectado o interesado un medio sencillo y gratuito que en ningún caso podrá suponer un ingreso adicional para el responsable del fichero o tratamiento ante el cual tales derechos se ejercitan. Además queda regulado expresamente el Derecho de oposición.

Transferencias internacionales de datos. En lo que a esto respecta, además de incorporar las previsiones de la controvertida Instrucción 1/2000 de la AEPD (parte de cuyo contenido fue anulado por el Tribunal Supremo en su sentencia de 25 de septiembre de 2006)[62], el nuevo Reglamento clarifica los criterios y procedimientos para su realización y/o autorización, en su caso.

Medidas de seguridad en el tratamiento de datos de carácter personal. El Reglamento trata de ser concretamente riguroso en la asignación de los niveles de seguridad, los cuales se ven incrementados con relación a los previamente exigidos por el Reglamento de Medidas de Seguridad.

.

[62] Sentencia del Tribunal Supremo, de 25 de septiembre de 2006, sobre la Instrucción 1/2000 de la Agencia de Protección de Datos sobre transferencias internacionales de datos. *"El Tribunal Supremo, ratifica en casación una Sentencia de la Audiencia Nacional, por la que se ha anula parte de la Instrucción1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos. Se impugnaron varias normas contenidas en la citada Instrucción 1/2000 de la Agencia Española de Protección de Datos que regula las transferencias internacionales de datos de carácter personal."*

CAPITULO 1

CAPITULO 1 - EQUILIBRIO ENTRE INFORMACIÓN Y SEGURIDAD NACIONAL. O COMO EL "REFORZAMIENTO DE LA SEGURIDAD" ANTE EL TERRORISMO, PUEDE PONER EN DUDA EL DISEÑO DEL ESTADO CONSTITUCIONAL Y DEMOCRÁTICO DE DERECHO

1. INTRODUCCIÓN

Los riesgos globales enfrentan a los Estados a un nuevo entorno estratégico cada vez más abierto e incierto que genera una sensación de inseguridad. Las medidas a adoptar pueden ser de distinta naturaleza, pero casi todas ellas han venido auspiciadas por la necesidad de garantizar la seguridad nacional. La restricción de las libertades desde los acontecimientos del 11-S y los siguientes grandes atentados terroristas, han desdibujado los esquemas tradicionales del binomio libertad / seguridad, han coadyuvado a reforzar este segundo concepto en detrimento del primero[63]. *El miedo al terrorismo global no puede dar lugar a que los Estados al sentirse amenazados actúen sin el debido respeto a los derechos fundamentales, legislando de forma excepcional.*[64] *El miedo se convierte en un generador de políticas que olvidan los espacios de libertad, haciendo primar la seguridad.* [65] La Lucha contra el terrorismo debe llevarse a cabo siempre dentro de los límites del estado de derecho y de la democracia constitucional. *El miedo, la sensación de inseguridad, la obsesión por la seguridad total tras brutales masacres, si bien puede aumentar los controles policiales o las intervenciones preventivas, no se puede ignora que los titulares de derechos fundamentales, inalienables, inviolables son inderogables*[66]. En este orden de cosas es conveniente recordar la Decisión-Marco del Consejo de la Unión Europea, de 13 de junio de 2002,

[63] Sobre las diferentes respuestas ofrecidas en la lucha contra el terrorismo internacional tras el 11-S puede verse, entre otros, el trabajo KENT R (2014): «The 9/11 effect in comparative perspective: some thoughts on terrorism in Canada, Spain and the United States», en REVENGA SÁNCHEZ, M (Director), Terrorismo y Derecho bajo la estela del 11 de septiembre, Valencia, Tirant lo Blanch, pp. 21-60.

[64] Citado en PÉREZ FRANCESCH, J.L. /GIL MARQUEZ, T; El terrorismo global, UOC, Barcelona, 2015.p.40

[65] CURBET, J.: Temeraris atemorits. L'obsessió contemporània per la seguretat, Girona, CCG Edicions, 2007.

[66] ver RUIZ MIGUEL, C (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», Revista de Derecho Comunitario, n.º 14, pp. 7-43.

(reformada en 2008), en materia de lucha contra el terrorismo, que intenta definir las reglas para homogeneizar la prevención y represión de los delitos de terrorismo por los Estados miembros, preocupándose al fin por respetar los derechos fundamentales[67]. La coordinación policial y judicial, mediante la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002 y denominada como euro-orden de extradición, ha permitido aplicar medidas eficaces de lucha desde las estructuras jurisdiccionales sobre sujetos vinculados con el terrorismo o con la criminalidad transnacional[68].

2. COMO EL "REFORZAMIENTO DE LA SEGURIDAD" ANTE EL TERRORISMO, PUEDE PONER EN DUDA EL DISEÑO DEL ESTADO CONSTITUCIONAL Y DEMOCRÁTICO DE DERECHO

Hoy se nos plantean dudas razonables sobre el mantenimiento de los esquemas institucionales del Estado de Derecho en su versión anterior al desarrollo de dichas medidas para luchar contra las nuevas versiones del fenómeno terrorista, o contra la criminalidad organizada transnacional, como graves problemas globales, con lo que entendemos que en ocasiones *se ha aprovechado el contexto para extremar de paso medidas tradicionalmente consideradas como extraordinarias, normalizándolas y así primar el principio de eficacia en la reacción ante posibles amenazas normalizando las medidas de excepción*[69]. En similar sentido Revenga Sánchez aludiendo que *"lo que dota de sentido a las medidas excepcionales es su carácter limitado en el tiempo y su función de instrumento para la recuperación de la normalidad"*[70].

El miedo al terrorismo puede originar que los Estados amenazados por el mismo sufran una "política del miedo", una sensación de

[67] Garantizados por el Convenio Europeo de Derechos Humanos y las Libertades Fundamentales, y la Carta de Derechos Fundamentales aprobada en Niza en 2002 e incorporada al Tratado de Lisboa en 2009.

[68] Vease comunicación de la Comisión al Parlamento Europea, al Consejo y al Comité Económico y Social Europeo y al Comité de las Regiones, bajo el título: "Prevenir la radicalización hacia el terrorismo y el extremismo violento: una respuesta más firme de la UE", de 15 de enero de 2014

[69] VERGOTTINI, G. D., Guerra y Constitución, Nuevo conflicto y defensa de la democracia, Il Mulino, Bologna, 2004, p. 21.

[70] REVENGA SÁNCHEZ., M., Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo. Parlamento y Constitución, n.20,2006-2007, p.61

"emergencia constante", constituyendo ésta situación el caldo de cultivo para legislar de forma excepcional, produciéndose así un verdadero proceso de marginalización de los derechos fundamentales. El miedo deviene así un generador de políticas que olvidan los espacios de Libertad, primando la seguridad. *La lucha contra el terrorismo no puede renunciar a dos requisitos ineludibles: el uso de medios no terroristas y el respeto al marco que impone la democracia constitucional*[71]

La *política de seguridad nacional* ha pasado a ser objetivo principal de la política judicial, en perjuicio de los derechos civiles y las garantías constitucionales. Como ha escrito Miguel Revenga, "*lo que llaman en los Estados Unidos "guerra contra el terrorismo" ha producido ya allí ciertas transformaciones en un modo de concebir la libertad política con una tradición de más de doscientos años"*[72]. Se ha creado una inteligencia nacional ampliada, que se extiende a todo tipo de información, con independencia de la fuente de la que proceda y que incluye información obtenida dentro y fuera de Estados Unidos, bajo el argumento de la defensa de la seguridad nacional[73] y en donde la tecnología al servicio de la vigilancia, hace que nuestra vida sea "transparente". La vigilancia afecta a todos los resortes de la vida actual, y llega un momento que ya no depende directamente de técnicas de procesamiento en manos del hombre, sino de máquinas a las que hay que controlar muy de cerca para que no acaben con la libertad humana[74].

2.1. Los principios que rigen el tratamiento de datos

El descubrimiento de escuchas masivas en el extranjero por parte de la agencia estatal de información NSA, y los escándalos por la revelación de secretos (casos Assange y Snowden) no ha generado más que incertidumbre

[71] WALZER, M., Terrorismo y Guerra Justa, Breus CCBB, Barcelona 2006, p.22
[72] REVENGA SÁNCHEZ., M., Garantizando la libertad y la seguridad …ob cit p.59
[73] Véase; AKERMAN, B: Antes que nos ataquen de nuevo. La defensa de las libertades en tiempos de terrorismo, Barcelona, Península, 2007; VERVALE J.: La legislación antiterrorista en Estados Unidos, ¿Inter arma silent leges?, Buenos Aires, Ediciones del Puerto, 2006. Citados en PÉREZ FRANCESCH, J.L. /GIL MARQUEZ, T; El terrorismo global, UOC, Barcelona, 2015.
[74] WHITAKER, R., El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad, Paidós, Barcelona,1999, p.11.

y desconfianza en amplios sectores de la población mundial. En el espionaje masivo de datos el ciudadano siente que el halo de privacidad con el que actúa e interactúa en su vida privada —y que es lo que le hace sentirse en libertad—está en peligro. Es cuando la pretendida búsqueda de la seguridad nacional acaba erosionando la «seguridad» que uno tiene en que hay un espacio en el que puede actuar sin controles y que hay una información que corresponde a ese espacio privado y que no goza de mayor relevancia o de la que no se pueden derivar mayores consecuencias. El conjunto de metadatos que se pueden almacenar sobre los ciudadanos es incalculable y puede ir desde una información muy sensible (ej. datos sobre salud) hasta otros datos que aisladamente considerados pudieran parecer no tener gran valor, como por ejemplo quién es el titular de un determinado móvil.

Cabe plantearse como interpreta Serra Cristóbal, *si del tratamiento de estos datos se puede producir una invasión en mi vida privada, dado que la jurisprudencia y numerosos textos supranacionales han considerado el tratamiento de los datos de carácter personal como una cuestión en la que puede verse afectado el ámbito de la intimidad/privacidad*[75] *del individuo*[76]. Si, además, se cruzan determinados datos de tráfico (identificación de llamadas, interlocutores en mensajes electrónicos…) y se tratan los mismos mediante determinados programas o técnicas informáticas que permiten conocer los interlocutores en una comunicación electrónica o incluso el contenido de la comunicación misma, podría quedar menoscabado el derecho a la inviolabilidad del secreto de las comunicaciones. Es indudable que, de un modo u otro, la recolección y almacenamiento de datos sobre comunicaciones, —que, entre otros, se produce por los servicios de inteligencia—, puede ir más allá de la mera recolección de datos o incluso tratarse de un control prospectivo del contenido mismo de las comunicaciones. Los servicios de inteligencia durante sus actividades de vigilancia,[77] deben velar por el respeto a la

[75] Sobre el ámbito de la privacidad o vida privada, vease, MARTÍNEZ MARTÍNEZ, R., (2005): Una aproximación crítica a la autodeterminación informativa, Madrid, Civitas, pp. 35-44.

[76] Vease RUIZ MIGUEL, C., (2003): «El derecho a la protección de los datos personales …ob cit, pp. 7-43.

[77] El sistema de escuchas telefónicas SITEL utilizadas por las fuerzas de seguridad del Estado y por los servicios del Centro Nacional de Inteligencia españoles es un avanzado sistema electrónico que permite interceptar y grabar en tiempo real cualquier conversación telefónica, correo electrónico o

legalidad vigente y a que el tratamiento de los datos goce de todas las garantías, —máxime, cuando afectan a la intimidad y más aún, si interfieren en el secreto de las comunicaciones—.

Cuando se trata de recabar datos derivados de comunicaciones que puedan afectar al secreto de éstas (escuchas telefónicas o electrónicas), nuestra Constitución exige la autorización de un juez, sin necesidad de distinguir entre interceptaciones individuales de comunicaciones o vigilancia masiva de comunicaciones (art. 18.3 CE). Y cuando dichos controles tienen que ser realizados por los servicios de inteligencia en el marco de sus funciones, la Ley Orgánica 2/2002, reguladora del control judicial previo del Centro Nacional de Inteligencia, indica que «el Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro».

Además, el TEDH ha realizado también un loable trabajo de protección de los derechos humanos en el marco de la lucha contra el terrorismo y, en concreto, en la protección de intimidad/privacidad cuando se llevan a cabo programas de vigilancia general o interceptaciones estratégicas, exigiendo no solo una habilitación legal, sino una previsión legal que sea precisa y respetuosa con los derechos fundamentales[78].

De las regulaciones jurídicas anteriores podemos afirmar la necesidad ineluctable de que la lucha contra el terrorismo en sus diversas manifestaciones se debe realizar dentro de los límites del Estado de Derecho y de la democracia constitucional. La doctrina del Tribunal Europeo de

---

mensaje de móvil, además de almacenar en formato digital todos los datos de esas comunicaciones para su posterior análisis. En todo caso, en principio, este sistema de vigilancia sólo puede ser utilizado con autorización judicial previa. Una descripción técnica de este sistema pude encontrarse en la STS 250/2009, de 13 de marzo. Citado en; SERRA CRISTÓBAL, R., "La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional". En *Revista de Derecho Político* N.º 92, enero-abril 2015, p 99.

[78] SSTEDH asunto; Valenzuela Contreras c. España, de 30 de julio de 1998; SSTEDH asunto; Padro Bugallo c. España, de 18 de febrero de 2003; SSTEDH asunto; Dulkarin Coban c. España, de 26 de septiembre de 2006 etc.

Derechos Humanos nos parece un buen referente para no caer en los abusos de la lucha contra la inseguridad y en especial el terrorismo: la garantía del derecho a la seguridad de los ciudadanos como deber del Estado, el respeto íntegro a los derechos y libertades reconocidos en el convenio, así como las garantías y controles precisos en las limitaciones o restricciones de los derechos de las personas (intimidad, secreto de las comunicaciones, protección de datos personales, privación de libertad) y aunque el Tribunal Europeo de Derechos Humanos ha reconocido que tal tipo de vigilancia prospectiva es a veces necesaria, exigiendo una previsión legal que la regule y que sea precisa y respetuosa con los derechos fundamentales, que exista proporcionalidad en el ejercicio de tales prácticas y una autoridad externa independiente que las supervise.[79]

En este sentido nuestra LO 15/1999, de protección de datos, no se aplica a los ficheros sometidos a la normativa sobre materias clasificadas o a los establecidos para la investigación del terrorismo (art. 2), los principios básicos que informan dicha Ley no dejan de tener pertinencia también en ese tipo de información recabada, almacenada y tratada por los servicios de inteligencia. Son principios que informan, entre otras cosas, cuándo se pueden recopilar datos, cuándo pueden cederse, o qué medidas de seguridad se adoptan para evitar el acceso de terceros. Estos principios son los de consentimiento, necesidad, y seguridad y todos ellos lógicamente dentro de la finalidad expresa por su autorización, para la que fueron recabados.

El principio de consentimiento, al igual que queda excepcionado por la Ley de Protección de datos para los ficheros de los cuerpos de seguridad del Estado, también queda excepcionado por la Ley reguladora del Centro

[79] SSTEDH asunto Murray c. the United Kingdom, 28 de octubre de1994, La Corte, en primer lugar, reiterar su reconocimiento de que el uso de información confidencial es esencial en la lucha contra la violencia terrorista y la amenaza que el terrorismo organizado representa para la vida de los ciudadanos y para la sociedad democrática en su conjunto. Esto no significa, sin embargo, que las autoridades investigadoras tengan carta blanca…». SSTEDH asunto Kopp C. Switzerland, 25 de marzo de 1998, «la grabación y otras formas de interceptación de conversaciones telefónicas constituyen una grave injerencia en la vida privada y la correspondencia y en consecuencia debe ser basada en una «ley» que sea particularmente precisa. Es indispensable contar con reglas claras y detalladas sobre el tema, sobre todo porque la tecnología disponible para ello se está haciendo cada vez en más sofisticada. Citado en; SERRA CRISTÓBAL, R., "La opinión pública ante la vigilancia masiva de datos… ob cit. p 101

Nacional de Inteligencia por el carácter secreto de toda información de inteligencia que generen dichos servicios (art. 5). Por lo tanto, no podemos decir que exista un derecho a acceder a los ficheros producto de la vigilancia prospectiva para inteligencia, como tampoco es necesario nuestro consentimiento para que se recaben esos datos.

El principio de necesidad, que exige que solo se puedan tratar datos cuando sean adecuados, pertinentes y no excesivos, obligaría a analizar en cada caso si estamos ante una actividad de recogida y tratamiento de datos que responda a un interés que justifique suficientemente la necesidad de llevarla a cabo, dado que es necesaria la justificación porque, como hemos indicado, de tal vigilancia y tratamiento de datos pueden derivarse posibles daños para los derechos de los ciudadanos, fundamentalmente para la salvaguarda de la privacidad/ intimidad y el derecho a la autodeterminación informativa de los titulares de tales datos, y en ocasiones para el secreto de las comunicaciones. Afirmando Serra Cristóbal, *que la recogida y tratamiento de datos personales y de comunicaciones, debiera producirse sólo cuando sea realmente necesario para la salvaguarda de la seguridad.*

El principio de seguridad exige que los datos con los que operan los servicios de inteligencia por su carácter sensible se salvaguarden mediante modos de encriptación. *La preocupación por la seguridad de las bases de datos sobre información clasificada ha estado presente en la UE desde hace años, en cuyo marco se han ido adoptando normas de seguridad para la protección de la información clasificada*[80]. La Orden Ministerial 76/2006, de 19 de mayo, la política de seguridad de la información del Ministerio de Defensa, mejoro las previsiones que existían en cuestión de seguridad de la información[81], mientras que el Real Decreto 3/2010, de 8 de enero, se centró en regular el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, generando confianza sobre los medios electrónicos en la relación entre el ciudadano y la Administración Pública.

[80] Decisión del Consejo 2001/264/EC, sobre las normas de seguridad del Consejo. Estas normas fueron modificadas en 2011, Decisión del Consejo 2011/292/UE, de 31 de marzo de 2011, sobre las normas de seguridad para la protección de la información clasificada de la UE. Citado en; Serra Cristóbal, R., "La opinión pública ante la vigilancia masiva de datos… ob cit. p 104

[81] Entre otras, las que se contemplaban en el Decreto 242/1969, de desarrollo de la Ley de Secretos oficiales; Orden Ministerial 12/1982, de 21 de octubre, del manual de seguridad industrial de las Fuerzas Armadas; Ley 15/1999, de protección de datos, ibídem p 105

2.2. La sociedad del control

La sociedad del siglo XXI camina hacia lo que Mattelart y Vitalis definen como un *"mundo vigilado", sociedad bajo el control de las nuevas tecnologías que hacen que nuestra intimidad sea mucho más permeable, donde cada vez se asienta más el principio del control,*[82] siguiendo lo afirmado por Silva Sánchez, *uno de los rasgos más significativos de las sociedades de la era postindustrial es la sensación general de inseguridad, esto es, la aparición de una forma especialmente aguda de vivir el riesgo*.[83] Las palabras pronunciadas por el Comisario europeo responsable del área de investigación P. Busquin, el 3 de febrero de 2004 no dejan duda a lo manifestado anteriormente *adoptar una cultura de la seguridad, movilizar a las fuerzas de la industria de la seguridad y la excelencia de la investigación europea, los acontecimientos han situado a la seguridad en la primera fila de las preocupaciones prácticas en Europa y en el mundo. La video-vigilancia globalizada como un medio de actuación policial "comporta una seria renuncia al modelo constitucional de garantía de las libertades.*[84].

No olvidemos que las tecnologías de la información vuelven transparentes nuestras vidas.[85] En palabras de Whitaker, en lo que alude como "arquitectura del control", *la interceptación de las comunicaciones sin autorización es posible ahora cuando se trate de investigaciones nacionales o internacionales cuya finalidad sea la salvaguarda de la seguridad nacional, para los datos registrados como mensajes de voz, o correos electrónicos,*[86] por lo que se deduce que todos los medios de comunicación que emplee el sospechoso pueden ser interceptados. Para analizar cuándo cabe tal limitación de las libertades para proteger a la seguridad nacional podrían ser útiles las

[82] MATTELART, A Y VITALIS.A., De Orwell al cibercontrol. Gedisa. 2015
[83] SILVA SANCHEZ, J M., La expansión del Derecho penal. Aspectos de la política-criminal de las sociedades postindustriales, 2ª ed., Madrid 2001. Citado en SERRA CRISTÓBAL, R… p.91
[84] Citado en GUDIN, F., La lucha contra el terrorismo en la sociedad de la información, Edisofer, Madrid, 2006, p.174
[85] La Directiva europea de 15 de marzo del 2006 obliga a los Estados miembros a almacenar durante dos años los datos de comunicación de sus ciudadanos.
[86] WHITAKER, R El fin de la privacidad: … ob cit, p.11.

reflexiones de Rawls sobre la llamada «regla del peligro claro y presente»[87]. Tal y como nos traslada Serra Cristóbal, aplicando análogamente la teoría de Rawls, *a la limitación de otros derechos ante un peligro claro y presente como lo supone el terrorismo internacional*.

Esta teoría, ya esgrimida por el Tribunal Supremo norteamericano diciendo que, *en cada caso, (los tribunales) deben preguntarse si la gravedad del mal reducida por su improbabilidad, justifica tal invasión de (la libre expresión) como la necesaria para evitar el peligro*[88]. Según esta doctrina, basta con que el mal probable sea suficientemente. Es necesario, por tanto, siguiendo a la citada autora, *que se trate de una situación de emergencia en el que se plantea una amenaza presente o previsible de grave perjuicio, pudiendo limitarse el contenido de un derecho, si ello es necesario para evitar una pérdida mayor y más significativa, bien directa o indirecta, de esas libertades*. Por lo tanto, también a nuestro juicio, solo cuando exista una probabilidad razonablemente constatable de que se produzca un daño en la seguridad de los ciudadanos a través de posibles ataques terroristas, cabría adoptar medidas que limiten o perjudiquen los derechos de los ciudadanos.

3. LAS NUEVAS POLÍTICAS EN LA LUCHA CONTRA EL TERRORISMO

En los Estados Unidos, "las medidas antiterroristas han provocado que muchas autoridades locales rechacen la aplicación de parte de la legislación "convencional" y sostengan –como el Fiscal general Ashcroft- que la política de seguridad nacional ha pasado a ser objetivo principal de la política judicial, en perjuicio de los derechos civiles y las garantías constitucionales"[89]. Según Revenga, *lo que llaman en los Estados Unidos "guerra contra el terrorismo", ha producido ya allí ciertas transformaciones en un modo de concebir la libertad política con una tradición de más de doscientos años* [90].

[87] RAWLS, J (ed. 1996): Sobre las libertades, Barcelona, Paidós, pp. 97 y ss. Citado en SERRA CRISTÓBAL, R… p.92
[88] Caso Dennis v. United States, 341 U. S. 494 en 510, cit. 183 F. 2, en 212. ibidem… p.92.
[89] Citado en PÉREZ FRANCESCH, J.L. /GIL MARQUEZ, T; El terrorismo global, UOC, Barcelona, 2015.p.75
[90] REVENGA SÁNCHEZ, M., Garantizando la libertad y la seguridad de los ciudadanos en Europa:

Estas medidas incidieron en la antesala de la reconsideración de derechos fundamentales como libertad y seguridad personales, aumentándose el tiempo de duración de la detención preventiva, la tutela judicial efectiva, con la creación de tribunales de excepción, o el derecho a un proceso debido con todas las garantías al ser afectados los sistemas de recursos o pruebas, o el secreto de las comunicaciones telefónicas y a través de Internet, permitiendo la interceptación de comunicaciones telefónicas sin mandato judicial[91].

La Comisión creada en EEUU a raíz de los ataques del 11-S, instaurada a finales de 2002, elaboró un exhaustivo y completo catálogo de las circunstancias que los produjeron. Esa Comisión hizo públicas sus conclusiones a finales de julio del 2004, entre las que se incluían 41 recomendaciones, en su mayoría dirigidas a la Intelligence Community. Todo este proceso cristalizó en la Intelligence Reformand Terrorism Prevention Act del 2004 (IRTPA). En ella, se contiene una definición de inteligencia nacional ampliada, que se extiende a todo tipo de información, *con independencia de la fuente de la que proceda y que incluye información obtenida dentro y fuera de Estados Unidos, comprendiendo de manera especial la relativa a la seguridad nacional*[92].El presidente Bush el 26 de octubre el Presidente sancionó la Patriot Act. Se trata de una ley extensa y compleja que confiere inusuales poderes ejecutivos a estructuras operativas de control y a los servicios de inteligencia, derivando esta misma a la adopción en varios Estados de Fellow Patriot Act, que han introducido previsiones similares en materia de registros, embargos, poderes especiales y excepcionales del gobernador[93].

La Patriot Act consta de diez Títulos que modifican unas 15 leyes federales ya existentes, entre ellas, el Wiretap Statute, el Computer Fraud and Abuse, el Foreing Intelligence Surveillance Act, el pen Register and

---

Nobles sueños y pesadillas en la lucha contra el terrorismo. Parlamento y Constitución, n.20,2006-2007, p.59.

[91] ÁLVAREZ, E Y GONZÁLEZ, H., Legislación terrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales, Real Instituto Elcano, Área de Terrorismo Internacional, ARI n.7/2006 Madrid,2006, p.2. Citados en PÉREZ FRANCESCH, J.L. /GIL MARQUEZ, T; ob cit p.102

[93] VERVAELE, J., La legislación antiterrorista en Estados Unidos…ob cit, p.12.

Trap and Trace Statute, the Immigration and Nationality Act, el Mioney laundering Act y el Bank Secrecy Act En su Título II se amplía notablemente la posibilidad de investigación digital, sin exigir en todos los supuestos la autorización judicial. La interceptación de las comunicaciones sin autorización es posible ahora cuando se trate de investigaciones nacionales o internacionales cuya finalidad sea la salvaguarda de la seguridad nacional, para los datos registrados como mensajes de voz, o correos electrónicos. La Patriot Act no exige órdenes de interceptación ni siquiera se requiere la autorización para la interceptación de comunicaciones de sujetos sospechosos de haber cometido abusos informáticos. Todos los medios de comunicación que emplee el sospechoso pueden ser interceptados, y quien lleve a cabo la interceptación no debe quedar identificado en la solicitud ni en la orden de interceptación.

Las repercusiones de la Patriot Act también se han dejado notar en el ámbito de la protección de fronteras y leyes de inmigración. En estas áreas se amplían de 24 horas a 7 días el plazo para comunicar los motivos de la detención administrativa. En el plazo de estos 7 días, el interesado debe ser acusado de un delito o bien ser conducido ante el Ministerio Público en el procedimiento de expulsión. Sin embargo y por motivos de seguridad nacional el Fiscal general puede ampliar el plazo de detención a 6 meses y prorrogarlo varias veces. Amparados en esta legislación, el Fiscal general y el INS (Inmigration and Naturalization Service) ostentan un poder de detención a largo plazo sin precedentes, sin posibilidad de defensa y sin obligación de declarar expresamente en qué se basa con exactitud la amenaza para la seguridad nacional. *La política antiterrorista desarrollada por los Estados Unidos ha supuesto en los últimos años un profundo cambio que ha afectado también a las reglas del ordenamiento de la ONU al justificar con la máxima amplitud el recurso a la fuerza e incluso en casos extremos a la "guerra preventiva", como se teoriza en la doctrina estratégica de Estados Unidos* (The Nacional Security Strategy of the United States of America, septiembre 2002)[94].

En similar sentido, la política antiterrorista seguida por el Reino Unido en los últimos tiempos ha merecido la crítica del Comisario de Derechos

[94] VERGOTTINI, G, D., Guerra y Constitución... ob cit.pág. 21.

Humanos del Consejo cuando el Primer Ministro Tony Blair presentó un proyecto de ley sobre seguridad, crimen y antiterrorismo (Antiterrorism, Crime and Security Act) que supuso la petición a la Cámara de los Comunes de la derogación del art. 5 de la Convención Europea de los Derechos Humanos y Libertades Fundamentales, que garantiza el derecho a la libertad y prohíbe la detención sin proceso judicial, en base a lo dispuesto en el artículo 15 de la Convención Europea que permite que los Gobiernos puedan derogar el citado artículo en tiempos de guerra o emergencia pública. Exponen Pérez Francesch, y Gil Márquez, *que la referida norma legal, una vez aprobada, supone un aumento importante de los poderes de policía por cuanto esta puede acceder sin control judicial alguno a interceptar los números de teléfono a los que llaman los vigilados y, en el ámbito de las garantías procesales*, sin embargo, esa Ley antiterrorista del 2001 fue declarada nula por el Tribunal de la Cámara de los Lores por ser incompatible con el Convenio Europeo de Derechos Humanos al permitir la detención de sospechosos de terrorismo de una manera que discriminaba en materia de nacionalidad o estatus de inmigración, al haberse recluido en cárceles británicas a nueve ciudadanos extranjeros sospechosos de terrorismo durante tres años sin proceso judicial, aunque ya previamente la Comisión de Apelación Especial de Inmigración de 2002 había declarado que era injustamente discriminatoria con los extranjeros que vivían en el reino Unido[95].

Posteriormente, el 11 de marzo del 2005, sería aprobada en el Reino Unido la Ley de Prevención del Terrorismo (Prevention Terrorism Act), aplicable tanto a los nacionales como extranjeros, la cual ante la imposibilidad de detener a los sospechosos de delitos de terrorismo sin una decisión judicial, introduce la figura de las llamadas "órdenes de control", que permiten vigilar a los extranjeros, controlar sus movimientos e incluso arrestarlos en su domicilio *La Ley antiterrorista Alemana, permite el arresto domiciliario sin cargos de sospechosos terroristas y una serie de "medidas de control", como el toque de queda, la vigilancia con medios electrónicos o la*

[95] Citado en PÉREZ FRANCESCH, J.L. /GIL MARQUEZ, T; El terrorismo global, ob cit, 2015.p.46

prohibición de usar Internet.[96]. A diferencia de la Ley de 2001, no distingue en su aplicación entre ciudadanos británicos y extranjeros, para evitar el argumento utilizado por la Cámara de los Lores cuando afirmó que la Ley de 2001 discriminaba entre uno y otros, en su aplicación. Tanto la ley del 2001 como la del 2005 a juicio de Amnistía Internacional, contienen disposiciones de amplísimo alcance que contravienen la legislación de derechos humanos y que han producidos abusos graves. El 11 de junio de 2008 el Gobierno del Reino Unido, veía por decreto ampliado el tiempo máximo de detención para sospechosos de terrorismo sin cargos de 28 a 42 días. No cabe duda de que todo lo expuesto comporta un ataque frontal a los postulados sobre los que se cimienta el Estado de Derecho, que se refleja en la disminución de las garantías hasta ahora consagradas, a través de los derechos fundamentales básicos. *Asistimos a un momento crucial en la defensa de las libertades por cuanto los postulados en los que se asienta la lucha contra el terrorismo en EEUU y Reino Unido, como hemos observado, dejan a la deriva el barco de las libertades y de los derechos humanos*[97].

En Alemania con la aprobación el 19 de diciembre del 2008 por parte del parlamento alemán de la nueva ley de la BKA (policía criminal) vio ampliadas las competencias policiales, posibilitando "en casos de urgencia" el espionaje on line de ordenadores, sin necesidad de autorización judicial, mientras que, en sintonía con el resto de países de la unión, las compañías de telefonía deben mantener seis meses inalterables sus bancos de datos por si la policía necesitase recurrir a ellos. Son muy interesantes las reflexiones del filósofo alemán Meter Sloterdijk cuando e relación a esta aprobación manifestó que *lo que caracteriza nuestra época es el triunfo de la seguridad sobre la libertad. Los ciudadanos se han convertido en súbditos de la seguridad. La libertad es víctima de nuestro siglo.*[98]

Por su parte, la nueva Ley antiterrorista aprobada en Francia en 2005 autorizó la videovigilancia en los transportes públicos, en las estaciones, Ministerios, comercios, sinagogas, iglesias y mezquitas. La Policía tiene acceso directo a las imágenes. La nueva Ley aprobada no sólo aborda la

[96] ALVAREZ, E., y GONZÁLEZ, H., ob. cit.pág.5
[97] PÉREZ FRANCESCH, J.L. y GIL MARQUEZ, T; ob cit.p.46
[98] ibidem. p 97

videovigilancia sino que además establece la obligación de que los operadores de telecomunicaciones conserven durante un año los contenidos de las conexiones a Internet, las conversaciones telefónicas de los usuarios y especialmente, reforzando esa inspección en los cibercafés. Los propietarios están obligados a conservar esos datos de transmisión. Los teléfonos celulares también son objeto de vigilancia por esta ley. Además, las compañías aéreas, ferroviarias y marítimas deben guardar los datos de sus clientes al menos durante doce meses. Asimismo, la ley amplía el plazo de presentación de los detenidos ante la Justicia de cuatro a seis días. La referida ley supone también, la posibilidad de que los servicios policiales puedan instalar sistemas de vigilancia fotográfica de vehículos, fotografiar a sus ocupantes y guardar las imágenes durante ocho días sin tener que pedir un mandamiento judicial. En este orden de cosas, hemos de recordar que la Directiva europea de 15 de marzo del 2006 obliga a los Estados miembros a almacenar durante dos años los datos de comunicación de sus ciudadanos.

4. REFERENCIAS

AKERMAN, B. (2007). *Antes que nos ataquen de nuevo.* La defensa de las libertades en tiempos de terrorismo, Barcelona, Península,

ALVAREZ CONDE, E y GONZALEZ, H. (2006*), Legislación terrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales,* Real Instituto Elcano, Área Terrorismo Internacional, *ARI* n. 7

CURBET, J. (2007).Temeraris atemorits. L'obsessió contemporània per la seguretat, Girona, CCG Edicions.

GUDIN, F. (2006), *La lucha contra el terrorismo en la sociedad de la información,* Madrid: Edisofer.

MARTÍNEZ MARTÍNEZ, R., (2005): Una aproximación crítica a la autodeterminación informativa, Madrid, Civitas.

MATTELART, A y VITALIS.A., (2015). De Orwell al cibercontrol. Gedisa.

PÉREZ FRANCESCH, J.L y GIL MARQUEZ, T; (2015).El terrorismo global, UOC, Barcelona,

RAWLS, J (1996): Sobre las libertades, Barcelona, Paidós.

REVENGA SANCHEZ, M. (2006*), Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo*, Parlamento y Constitución, n. 20.

REVENGA SÁNCHEZ, M (2007) (Director), Terrorismo y Derecho bajo la estela del 11 de septiembre, Valencia, Tirant lo Blanch

RUIZ MIGUEL, C (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», Revista de Derecho Comunitario, n.º 14

SERRA CRISTÓBAL, R., (2015) "La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional". En *Revista de Derecho Político* N.º 92, enero-abril

SILVA SANCHEZ, J M., (2001) La expansión del Derecho penal. Aspectos de la política-criminal de las sociedades postindustriales, 2ª ed., Madrid 2001.

VERGOTTINI, D (2004), *Guerra e costituzione. Nuovi conflictti e sfide alla democrazia*, Bologna:Il Mulino.

VERVALE J (2006), *La legislación antiterrorista en Estados Unidos, ¿Inter arma silent leges?*, Buenos Aires: Ediciones del Puerto.

WALTER, M.(2006), *Terrorismo y guerra justa*, Barcelona:Centre de Cultura Contemporanea de Barcelona.

WHITAKER, R.(1999) *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Barcelona: Paidós.

CAPITULO 2

CAPITULO 2 - EL USO DE DRONES COMO FACTOR DE INTELIGENCIA Y SU IMPACTO EN LA LEGISLACION DE PROTECCION DE DATOS DE CARÁCTER PERSONAL

1.- INTRODUCCIÓN

El empleo creciente de la inteligencia artificial mediante robots denominados Drones, representa un sector en expansión que todavía no tiene bien definidos sus límites, pudiendo ser estos utilizados en múltiples tareas lúdicas, comerciales o profesionales, pero que coinciden todas ellas en una herramienta con un alto potencial [99], En cuanto a lo notorio que ha sido su rápida evolución y sus múltiples posibilidades, donde se comprueban las diferentes aplicaciones en el sector militar[100] o incluso policial[101], mientras que en el sector civil, se discuten las posibilidades que

[99] La Comisión Europea, estima que el sector de los Drone, podrá generar aproximadamente 150.000 empleos y obtendrá alrededor de 15.000 millones de euros hasta el año 2050, mientras que la (FAA) considera que el mercado de los drones domésticos podría generar unos 90.000 millones de dólares únicamente en la próxima década.

[100] Segun HALLA, A.R., COYNEA, C.J., The political economy of drones. Routledge - Taylor & Francis Group. 2013. El uso de ingenios aéreos no tripulados, en los ámbitos militar, de la seguridad o de la inteligencia se remonta al año 1849 con la utilización de globos aerostáticos no tripulados para bombardear Venecia, o con el mismo objetivo en la Guerra Civil Americana de 1860, aunque podríamos considerar como el primer vehículo que se acomode de algún modo a la denominación actual de UAV fue desarrollado por la marina estadounidense en 1915, mientras que fue en 1918, cuando el ejército USA desarrollo el Kettering Bug, una máquina voladora con giroscopio controlado. Finalizada la Primera Guerra Mundial, en la década de los 30, la Armada de los Estados Unidos llevó a cabo experimentos incluyendo técnicas de radiocontrol que procurasen mejorar la precisión de la que carecían cualquier ingenio anterior, logrando finalmente en 1938 incluir a los "UAVS" en la práctica de la artillería antiaérea. La Segunda Guerra Mundial produjo una serie de innovaciones y experimentos, los cuales hacen que el desarrollo de misiles y \UAVs" evolucionen claramente. A partir de las décadas de 1950 y 1960, según, WATTS, A.C., AMBROSIA, V.G., HINKLEY, E.A., Unmanned aircraft systems in remote sensing and scienti_c research: Classi_cation and considerations of use. Remote Sensing 2012. los drones empiezan a ser considerados para otras tareas, como obtener y recopilar información del enemigo en áreas peligrosas. El Firebee Drone fue utilizado para ello en la Guerra de Vietnam con relativo éxito. Las tareas destinadas a los drones se caracterizaban por ser: "the three Ds: dull, dirty and dangerous work", donde la presencia de un piloto humano corría con desventaja. Entre 1970 y 1980 la NASA desarrolló aviones no tripulados para la toma de muestras atmosféricas y en 1990 con otros programas para el desarrollo de "UASs" para el soporte a investigaciones científicas. Mientras que en el ámbito militar los avances se fueron dando por la Fuerza Aérea de los Estados Unidos mediante los "UAVS", Global Hawk, cuya misión se basa en trabajos de inteligencia, vigilancia y reconocimiento y el Predador el cual tiene capacidad ofensiva, estando actualmente ambos en vigencia y funcionamiento.

[101] North Dakota police will be free to fire 'less than lethal' weapons from the air thanks to the

brindan las altas capacidades de estos aparatos y se enfatiza en su necesaria acomodación jurídico legal, "concreta".

El descubrimiento y potenciación de uso de las aeronaves no tripuladas en la última década ha supuesto un nuevo paradigma legal y operativo, no ajeno a las críticas sobre las capacidades de estas aeronaves, y que tienen la capacidad de abarcar protocolos de funcionamiento tanto en labores civiles como militares, en donde estas últimas, pueden circunscribirse a labores propias de la inteligencia, o a la participación directa en los conflictos, representando ambos campos de actuación un sector en expansión que todavía no tiene bien definidos los límites de su potencial, si bien, pueda resultar notoria su aplicación en el sector de la inteligencia y la seguridad, constatándose como un hecho plausible, resultar un elemento determinante en la lucha contra el terrorismo internacional, mientras que su introducción en la sociedad civil, a pesar de las múltiples bondades y usos diversos, plantean una serie de cuestiones que al momento, ven necesaria su armonización, discutiéndose en este artículo, las posibilidades que brindan las altas capacidades de estos aparatos. El uso que se puede hacer de estos ingenios aéreos es muy variado como podremos observar, analizando en este artículo su empleo con fines de seguridad y la utilización con fines de uso civil.

Los Drones, UAV y RPA son las distintas denominaciones con las que los medios identifican a estos robots aéreos y que todos ellos tienen el denominador común de ser aeronaves no tripuladas. Estos conceptos si bien pueden aludir en conjunto al fenómeno, no significan lo mismo. El termino drone, es comúnmente empleado en el sector aeronáutico para denominar a los vehículos aéreos no tripulados, y circunscritos generalmente al ámbito de usos militares, pero en estos casos para ser correctos en la conceptualización del término, se debería generalmente utilizar las siglas UAV[102], como siglas que identifican en inglés Unmanned

influence of Big Drone. http://www.thedailybeast.com/articles/2015/08/26/first-state-legalizes-armed-drones-for-cops-thanks-to-a-lobbyist.html

[102] Vehículo aéreo no tripulado, esto es, no lleva personal como operador a bordo. Los vehículos aéreos no tripulados (UAV) incluyen solo aquellos vehículos controlables en los tres ejes. Este término es únicamente alusivo sobre el aparato que vuela, ya que si estamos refiriéndonos al sistema completo –o sea el avión más el sistema de control- se habla de UAS, Unmanned Aerial System, o sistema aéreo no tripulado, que comprenderá tal y como detalla la citada Orden PRE/1366/2010, de

Aerial Vehicle como, vehículo aéreo no tripulado. Por ello, lo más correcto cuando hablamos de Drones, seria denominarlos concretamente UAV, aunque como veremos se ha normalizado el término de RPA[103] y que detallaremos más adelante.

Es evidente que todavía falta consenso en las denominaciones por los diferentes estados sobre la conceptualización de cada tipo de aparato que comúnmente son englobados todos ellos bajo el término drone[104], siendo una prioridad a nivel tanto estatal como internacional, lograr un consenso que clarifique no solo la terminología sobre cada uno de ellos sino las características que acompañan al término que se le dote, dado que su uso convencional civil, como en usos de la seguridad o en cualquier uso militar

los elementos individuales del sistema UAV, que incluyen el vehículo aéreo no tripulado (UAV), la estación de control en tierra y cualquier otro elemento necesario para permitir el vuelo, tales como el enlace de comunicaciones o el sistema de lanzamiento y recuperación.» Las capacidades de un UAV serán:
a) Es capaz de mantenerse en vuelo por medios aerodinámicos
b) Es pilotado de forma remota o incluye un programa de vuelo automático.
c) Es reutilizable.
d) No está clasificado como un arma guiada o un dispositivo similar de un solo uso diseñado para el lanzamiento de armas.

[103] Son aeronaves pilotadas de forma remota, es decir, sin piloto, y que se conocen por sus siglas en inglés como "RPAS" (Remotely Piloted Aircraft Systems). La Orden PRE/1366/2010, de 20 de mayo, por la que se modifica el Reglamento de la Circulación Aérea Operativa, aprobado por el Real Decreto 1489/1994, de 1 de julio, ha introducido dos definiciones al respecto:
Vehículo aéreo no tripulado: Vehículo aéreo propulsado que no lleva personal como operador a bordo. Los vehículos aéreos no tripulados (UAV) incluyen solo aquellos vehículos controlables en los tres ejes. Además, un UAV:
a) Es capaz de mantenerse en vuelo por medios aerodinámicos.
b) Es pilotado de forma remota o incluye un programa de vuelo automático
c) Es reutilizable
d) No está clasificado como un arma guiada o un dispositivo similar de un solo uso diseñado para el lanzamiento de armas.
Sistema aéreo no tripulado: Comprende los elementos individuales del sistema UAV, que incluyen el vehículo aéreo no tripulado (UAV), la estación de control en tierra y cualquier otro elemento necesario para permitir el vuelo, tales como el enlace de comunicaciones o el sistema de lanzamiento y recuperación.

[104] El término "drone" se especula que está referido al zumbido constante de estos aparatos cuando están sobrevolando una zona, en BENJAMIN, M., *Drone Warfare. Killing by Remote Control*, Brooklyn, Verso, 2013, fully revised and updated, p. 13. También se especula en que se acuño esta denominación al hacer referencia a la limitada capacidad que tenían estos vehículos en ese entonces, además de su propiedad de desechable y fácil sustitución en comparación con aeronaves tripuladas, en SULLIVAN, J.M., ¿Evolution or revolution? rise of uavs. IEEE Technology and Society Magazine 25(3) 2006.

en determinado conflicto, no necesariamente armado, podría suscitar problemas legales entre sus usuarios y la legislación aérea de los estados.

Por ejemplo, para los casos de uso militar también se ha reconocido por parte de los expertos las siglas UCAV[105], (Unmanned Combat Aerial Vehicle), como término que alude al vehículo aéreo no tripulado de combate, siendo estos aparatos, capaces de portar armamento para atacar objetivos determinados, mientras que desde hace pocos años se ha generalizado el concepto de los RPA, (Remotely Piloted Aircraft), como término que alude a los aviones controlados de forma remota. El Real Decreto Legislativo 8/2014, de 4 de julio[106], incorporo una sección completa dedicada a las Aeronaves civiles pilotadas por control remoto, fijando las condiciones de explotación de RPAS, abordando exclusivamente la operación de aeronaves civiles pilotadas por control remoto de peso inferior a los 150 Kg y aquellas de peso superior destinadas a la realización de actividades de lucha contra incendios, búsqueda y salvamento. El Real Decreto atribuye al Ministerio de Fomento la competencia para la circulación aérea general (situaciones de crisis ordinarias como fenómenos naturales), atribuyendo al Ministerio de Defensa las competencias sobre la materia en situaciones extraordinarias o de emergencia.

El Real Decreto 8/2014, se transformó en la Ley 18/2014[107], de 15 de octubre, acotada igualmente que su predecesora con un carácter y vigencia

[105] Véase al respecto MELZER, N., Implications of the Usage of Drones and Unmanned Robots in Warfare, Directorate-General for External Policies of the Union, European Union, Brussels, May 2013, p. 6.

[106] Véase GUERRERO LEBRÓN, M. J., «La regulación transitoria de los operadores de aeronaves civiles pilotadas por control remoto», La Ley mercantil, 31 de julio de 2014, Editorial La Ley.

[107] Si bien la Ley 18/2014 si establece requisitos que regula tales como el peso máximo del aparato al despegue y clasifica los Drone pilotados por control remoto de peso inferior a los 150 kilos en tres categorías: 1. Drones de más de 25 kilos que no superan los 150 kilos: son las únicas aeronaves que deberán estar registradas en el Registro de Matrícula de Aeronaves y contar con un certificado de aeronavegabilidad emitido por la Agencia Estatal de Seguridad Aérea. El piloto necesitará un certificado básico o avanzado emitido por una organización de formación autorizada. (un certificado básico para volar dentro del alcance visual del piloto o certificado avanzado para volar más allá del alcance visual del piloto). 2. Drones de menos de 25 kilos y hasta 2 kilos: no necesitan estar inscritos en el registro de aeronaves ni disponer de un certificado de aeronavegabilidad, pero deberán emitir una comunicación previa de vuelo, así como una declaración responsable a la AESA con una antelación mínima de cinco días. El dron debe estar dentro del alcance visual del piloto y se requiere un permiso especial para la obtención de fotografías o filmaciones. 3. Drones inferiores a 2 kilos: son los únicos que pueden volar más allá del alcance visual del piloto pero sujetos al alcance de la

temporal, "hasta que el Gobierno determine reglamentariamente el nuevo régimen jurídico aplicable a los drones", donde cabe igualmente volver a mencionar para redondear esta espectro normativo en España, el pretérito régimen normativo que discurre en la Ley 48/1960, de 21 de julio, de Navegación Aérea (LNA), partiendo de un régimen general descrito en los artículos 150 y 151 de la citada Ley, modificada para establecer con carácter concluyente que los drones son aeronaves y como tales su utilización civil está sujeta a la legislación aeronáutica civil[108]. Esta Ley como indicamos, se modifica para establecer el marco jurídico específico para el uso y operación de las aeronaves pilotadas por control remoto, contemplando, conforme a lo previsto en la normativa de la Unión Europea sobre operaciones especializadas, la doble posibilidad de someter la realización de la actividad a una comunicación previa o a una autorización administrativa, aunque huelga decir que ninguna de las leyes mencionadas contiene una definición conceptual de dron, que parece verse satisfecha en el borrador no oficial del inminente (desde hace dos años) Nuevo Real Decreto[109] que regule las

emisión por radio de la estación de control. Aunque tampoco se exige certificado ni inscripción, debe emitirse un aviso de vuelo al resto de usuarios del espacio aéreo informando del lugar y hora en los que se volará. Además, debiéndose aclarar que según el art 50.2 Las aeronaves civiles pilotadas por control remoto cuya masa máxima al despegue exceda de 25 kg deben estar inscritas en el Registro de matrícula de aeronaves y disponer de certificado de aeronavegabilidad, quedando exentas del cumplimiento de tales requisitos las aeronaves civiles pilotadas por control remoto con una masa máxima al despegue igual o inferior. Además, todas las aeronaves civiles pilotadas por control remoto deberán llevar fijada a su estructura una placa de identificación en la que deberá constar, de forma legible a simple vista e indeleble, la identificación de la aeronave, mediante la designación específica y, en su caso, número de serie, así como el nombre de la empresa operadora y los datos necesarios para ponerse en contacto con la misma.

[108] Artículo 11 la Ley 48/1960 redactado por el apartado uno del artículo 51 de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia). "Se entiende por aeronave: a) Toda construcción apta para el transporte de personas o cosas capaz de moverse en la atmósfera merced a las reacciones del aire, sea o no más ligera que este y tenga o no órganos motopropulsores. b) Cualquier máquina pilotada por control remoto que pueda sustentarse en la atmósfera por reacciones del aire que no sean las reacciones del mismo contra la superficie de la tierra"

[109] Se supone que el próximo documento legislativo que regule la particularidad del uso civil de los Drone, en su borrador no oficial, este ya describe al Drone como "Aeronave pilotada por control remoto (RPA), refiriendo esta como, "aquella aeronave no tripulada, pilotada a distancia desde una estación de pilotaje remoto. Abundando igualmente respecto a un RPA como "Sistema de aeronave pilotada por control remoto (RPAS)» incluyendo el conjunto de características necesarias para su utilización como son, su estación o estaciones de pilotaje remoto conexas, los necesarios enlaces de mando y control y cualquier otro elemento de sistema que pueda requerirse en cualquier momento durante la operación de vuelo.

circunstancias del desenvolvimiento de los Drone y trate igualmente de armonizase con la normativa europea.

El régimen específico de las operaciones de los drones se establecerá por tanto, reglamentariamente y conforme al estado de la técnica, estando todavía inconcluso. No obstante, en tanto se procede a dicho desarrollo reglamentario, en el Real Decreto-ley 18/2014, de 15 de octubre[110], pero esta ley como hemos explicado anteriormente, regula exclusivamente la operación de drones de peso inferior a los 150 Kg y aquellos de peso superior destinados a la realización de actividades de lucha contra incendios y búsqueda y salvamento, dado que, en general, el resto de drones que no se sujeten a esta distinción de pesos y autonomía, estaría sujeto a la normativa de la Unión Europea[111].

[110] La Disposición Final Segunda de la Ley 18/2014, habilita al Gobierno para el desarrollo reglamentario futuro del régimen jurídico aplicable a las aeronaves civiles pilotadas por control remoto y "a la entrada en vigor de la referida norma reglamentaria quedará sin vigencia el contenido del artículo 50".puesto que la inclusión en la citada ley de medidas urgentes algunas de las funciones y características de utilización de los drones, como bien dice la ley acotando su inclusión, tal y como la propia ley describe, con ánimo de precisar (y no de regular), en donde, profundizando en esta "regulación" observamos que en la Sección 6ª, del capítulo I del Título II de la Ley, se regula el uso de aeronaves civiles pilotadas por control remoto, compuesta de un único artículo, esto es el 50, merece nuestra atención su párrafo 3º, letra d, apartado 7º, que obliga al operador de una aeronave no tripulada a contratar un seguro de responsabilidad civil que cubra la responsabilidad civil frente a terceros por daños que puedan surgir durante y por causa de la ejecución del vuelo", circunscribiéndose la responsabilidad del operador según esta "regulación en la Ley 18/2014, no solo a los daños susceptibles de ser causados por la aeronave, por un posible fallo técnico, o alteración del espectro eléctrico, (estas aeronaves operan en la misma banda que por ejemplo detonadores en minas a cielo abierto, controles de grúas torre en construcciones etc.), si no que se amplía esta responsabilidad, al objeto que aquí nos interesa, como establece el artículo 50.1.2 "el cumplimiento de lo dispuesto en este artículo no exime al operador, que es, en todo caso, el responsable de la aeronave y de la operación, del cumplimiento del resto de la normativa aplicable, en particular en relación con el uso del espectro radioeléctrico, la protección de datos o la toma de imágenes aéreas, ni de su responsabilidad por los daños causados por la operación o la aeronave", por lo que atendiendo a la norma de esta " Regulación", el operador es responsable civil directo de los daños, desplegando sus efectos en ámbitos como la privacidad, intimidad, y el derecho a la imagen,

[111] Con la actual legislación estaría prohibida la utilización de drones sobre núcleos urbanos o grupos de población (playas, conciertos o manifestaciones, espacios en general con una alta masificación de gente). Pudiéndose conceder autorizaciones puntuales por la autoridad competente. Con la limitación descrita, e independientemente de esta, los drones se pueden utilizar en trabajos aéreos como:

• Actividades de investigación y desarrollo;
• Tratamientos aéreos, fitosanitarios y otros que supongan esparcir sustancias en el suelo o la atmósfera, incluyendo actividades de lanzamiento de productos para extinción de incendios;
• Levantamientos topográficos aéreos;

Para tratar de dilucidar algún tipo de unanimidad respecto al fenómeno Drone, acudimos a la denominación que la Unión Europea describe, refiriéndose a estos como Drone a los vehículos aéreos de uso civil, mientras que la Organización de Aviación Civil Internacional (ICAO)[112] habla de estos aviones como RPAs y UAs, (Unmanned Aircraft), como término que alude al avión no tripulado y que la generalidad de los expertos denomina como hemos expuesto RPA, Remotely Piloted Aircraft, término que alude "al avión no tripulado que es pilotado de forma remota". Es por esto que insistimos en la necesaria normalización de los términos, pues se supone problemática la falta de legislación y conceptualización uniforme sobre drones, máxime cuando estos puedan tener uso y finalidad en seguridad.

Es notable el interés demostrado desde la Unión Europea cuando muestra su interés en elaborar una normativa que integre el fenómeno Drone en el espacio aéreo mediante la elaboración en septiembre del 2012, por parte de la comisión Europea del documento de trabajo "Hacia una estrategia europea para el desarrollo de las aplicaciones civiles de las aeronaves no tripuladas (RPAS)", al que le siguió en junio del 2013, de la hoja de ruta para la integración de los drones de uso civil en el sistema europeo de aviación, confeccionada por el Grupo Directivo Europeo sobre los Drones.

La Unión Europea mediante Eurocontrol[113] se articula como uno de los actores principales a la hora de plantear la agenda del desarrollo de los

• Observación y vigilancia aérea incluyendo filmación y actividades de vigilancia de incendios forestales e Infraestructuras;
• publicidad aérea, emisiones de radio y TV;
• operaciones de emergencia, búsqueda y salvamento;
• y otro tipo de trabajos especiales no incluidos en la lista anterior.

[112] La Organización de la Aviación Civil Internacional) publicó en 2011 a través de su Grupo de Estudio sobre Sistemas Aéreos no Tripulados (UASSG) la Circular 3281 como un inicio de regulación y de creación de SARPs (Standards and Recommended Practices); mientras que en 2015 a publicado el Documento 10019 o Manual sobre RPAS como una guía para los Estados y los operadores a la hora de armonizar las regulaciones con el fin de la integración de los RPAS en un espacio aéreo único y no segregado. www.wyvernltd.com/wp-content/uploads/2015/05/ICAO-10019-RPAS.pdf

[113] La Organización Europea para la Seguridad de la Navegación Aérea, Eurocontrol, está compuesta por 41 Estados que tienen como objetivo, desarrollar un sistema seguro, eficaz y coordinado del tráfico aéreo europeo. El listado que Eurocontrol facilita de normativas nacionales sobre drones

Drones en Europa[114], participando activamente dentro del Panel sobre RPAS de la OACI, en sus Grupos de Trabajo sobre Gestión de Tráfico Aéreo y el C2 Data Link. Tambien dentro del ámbito de la UE a través de la Comisión Europea en la integración de los RPAS, y a través de la Comunicación de la Comisión en abril de 2014 y llamada "Una nueva era para la aviación" que amparara el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible, como estrategia para impulsar el desarrollo del mercado europeo de drones[115], así como en la Declaración de Riga de marzo de 2015[116], así como la Resolución del Parlamento Europeo sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS), comúnmente conocidos como vehículos aéreos no tripulados (UAV), en el ámbito de la aviación civil, de 29 de octubre de 2015[117].

Los cinco principios rectores que establece la Declaración de Riga, que permitirán el uso de drones desde 2016 son los siguientes:

- Los drones deben ser considerados como un nuevo tipo de aeronave, apuntando a la necesidad de que estos sistemas sean "tratados como nuevos tipos de aeronaves con reglas proporcionales basadas en el riesgo de cada operación". En la explicación de este principio, sus

puede consultarse en https://easa.europa.eu/unmanned-aircraft-systems-uas-and-remotely-piloted-aircraft-systems-rpas.

[114] El desarrollo de los Drone en Europa según Eurocontrol, evidencia que distintos países contienen normativa propia, tales como Alemania, Austria, Bélgica, Croacia, Dinamarca, España, Finlandia, Francia, Holanda, Irlanda, Italia, Reino Unido, República Checa, Suecia y Suiza. En el caso de España, su regulación de 2014, se supone una normativa temporal mientras el legislador observa una nueva legislación que abarque las múltiples posibilidades de estas aeronaves.

[115] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL COM/2014/0207 final A new era for aviation Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0207

[116] RIGA DECLARATION ON REMOTELY PILOTED AIRCRAFT (drones) "FRAMING THE FUTURE OF AVIATION" Riga,6 March 2015
http://www.aerpas.es/wp-content/uploads/2015/03/EU_Riga-Declaration_150306.pdf?531a11

[117] La Agencia Europea de Seguridad Aérea (EASA) regula únicamente los drones de más de 150 kilos, dejando en manos de las autoridades aeronáuticas de los distintos Estados miembros, la reglamentación de los drones de peso inferior, así como la potestad de los vuelos experimentales, los vuelos gubernamentales tanto militares como no militares, según el reglamento (CE) no 216/2008, pero en la citada resolución se aboga por aunar coherentemente la regulación de los drones sin atender a su masa, para que de este modo sea exhaustivo el control ejercido sobre toda la unión, para toda clase de drones.

autores destacan que estos aviones no deben ser menos seguros que los convencionales –tripulados– de la aviación civil y que deben de estar sujetos a una regulación similar a la que ya se aplica en la aviación que sí lleva pilotos en sus aparatos.

- Las reglas europeas para la operación de drones deben desarrollarse con carácter inmediato. haciendo hincapié en que las "normas de la UE para la prestación segura de servicios con aviones no tripulados debe desarrollarse ahora". En él se destaca que estas reglas, incluidas las cualificaciones para las empresas operadoras y los pilotos de los drones, deberán ser desarrolladas a nivel continental por la Agencia Europea de Seguridad Aérea (Aesa) y basarse en la experiencia recopilada por los estados miembros. Los requisitos esenciales deberán armonizarse a nivel internacional al máximo posible. La necesidad de poner en marcha cuanto antes este marco normativo persigue ayudar al sector privado a tomar sus decisiones de inversión con el mayor conocimiento de causa.
- Deben desarrollarse tecnologías y estándares que faciliten la integración de los drones en el espacio aéreo europeo advirtiendo la Declaración en este punto, la importancia de que tanto la industria como las autoridades públicas realicen el necesario esfuerzo financiero que permita lograr y validar las tecnologías necesarias para lograr el uso seguro de aeronaves no tripuladas en los cielos del continente europeo.
- La aceptación pública de los drones es clave para el crecimiento de los servicios asociados a los drones, aludiendo a los peligros que los drones pueden representar para los derechos fundamentales como la privacidad y la protección de datos personales, que podrían verse amenazados por el uso de filmaciones de ámbitos particulares, por ejemplo. También incluye aspectos como las molestias que del ruido o la amenaza que su mal uso puede suponer para la seguridad.
- El operador del dron es el responsable de su utilización, apelando la Declaración que el "responsable" de la utilización de un avión no tripulado será su operador, de modo que cuando se cometa alguna irregularidad, como sobrevolar un área prohibida o moverse de

> manera insegura, las consecuencias legales caigan sobre el propietario u operador, que deberá ser inidentificable y sometido a una serie de seguros y de mecanismos de compensación para atender y resarcir los potenciales perjuicios por su uso.

Mientras que con arreglo a las normas de la organización de aviación civil internacional[118] para aeronaves tripuladas así como las diferencias operacionales, jurídicas y de seguridad entre operaciones de aeronaves tripuladas y no tripuladas operaran para integrar los UAS en el espacio aéreo no segregado y en aeródromos no segregados, debiendo haber un piloto responsable de la operación UAS, en donde en ninguna circunstancia la responsabilidad del piloto podrá sustituirse por tecnologías ciberautonomas en el futuro previsible. Según la ICAO, para reflejar mejor la condición de estas aeronaves que son realmente pilotadas, se introduce en el vocabulario la expresión "aeronave pilotada a distancia" (RPA). Una RPA es una aeronave pilotada por un "piloto remoto", titular de licencia, emplazado en una "estación de piloto remoto" ubicada fuera de la aeronave (es decir, en tierra, en barco, en otra aeronave, en el espacio) quien monitorea la aeronave en todo momento y puede responder a las instrucciones expedidas por el Control del tránsito aéreo (ATC), se comunica por enlace de voz o datos según corresponda al espacio aéreo o a la operación, y tiene responsabilidad directa de la conducción segura de la aeronave durante todo su vuelo.

En este sentido expone Oñate de Mora, que "parece reconocido por todos que drone y UAV/UAS suelen ser denominaciones para aparatos militares y RPA/RPAS para civiles. Pero que es importante saber que todos los RPA son UAV, ya que son vehículos aéreos no tripulados, pero no todos los UAV son RPA, ya que para ello deben estar controlados por una persona"[119].

---

[118]ICAO Cir 328, Unmanned Aircraft Systems (UAS) Order Number: CIR328 http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

[119] D. Manuel Oñate de Mora es presidente de la asociación española AERPAS de RPAS, http://www.lavozdegalicia.es/noticia/economia/2015/08/30/falta-marco-legal-sector-crezca-forma sana/0003_201508G30P28995.htm y en http://www.securityforum.es/pregunta-a-los-ponentes/drones-y seguridad-manuel-onate/

Respecto a la diferenciación de los "RPAS" estos pueden ser clasificados por varios aspectos entre ellos su arquitectura, su tamaño, su capacidad de carga, por su alcance y altitud, por los usos y otras características[120]. Se toma como referencia la clasificación propuesta por la OTAN, que como observaremos insiste en denominarlos UAV, cuando ya el consenso general es considerara los UAV, RPA, dicho esto, veamos como los define y en qué tipos de clases:

- Clase I. Los micros, mini y ligero "UAVS", tienen una gran facilidad de manejo por un solo operador, sin necesidad de pista de despegue y aterrizaje en espacios minúsculos. Aquí se encuentran los "VTOL", Vertical Take-Off & Landing o drones de despegue y aterrizaje vertical. Muchos de estos tipos de drones pertenecen a las aplicaciones del ámbito tactico. Pueden pesar entre 2 y 30 kilogramos.
- Clase II. Los "UAVS" tácticos y "MALE Medium-Altitude Long-Endurance, son más pesados, entre 150 y 1.500 kilos, vuelan a una altitud entre los 1000 y los 8000 metros y pueden diferir bastante en su autonomía de vuelo, siendo usados en operaciones militares. Los "MALES" usan tecnología más avanzada como conexiones vía satélite y, en algunos modelos, pueden permanecer en el aire durante cuarenta horas, aunque por ejemplo, un drone de la empresa Lockheed Martin - denominado "Stalker ", puede ser recargado desde tierra usando un rayo láser, lo que abre la puerta a que, en el futuro, teóricamente, un "UAV" pueda permanecer volando indefinidamente.
- Clase III. Los "UAVS" con mayor peso se agrupan con la denominación "HALE High-Altitude Long-Endurance", son grandes y pesadas plataformas que van desde más de 600 kg, pudiendo llegar hasta las doce toneladas y volar a una altitud máxima de 20.000 metros. Aunque su uso sigue siendo predominantemente militar también se utilizan en otros

[120] BARRIENTOS, A, et al., Vehículos aéreos no tripulados para uso civil. Tecnología y aplicaciones. Universidad Politécnica de Madrid. 2007.

> entornos como realización de mapas y observaciones atmosféricas y terrestres, uno de los más conocidos es el \Helios", operado por la NASA y que funciona con energía solar.

Observadas a vuelapluma algunas características para definir los conceptos y diferenciaciones que nos permitan establecer un acercamiento al fenómeno "drone", donde el uso de drones con fines militares es un proceso de carácter irreversible, tal y como ha señalado el Relator Especial ONU al afirmar que "los drones están aquí para quedarse"[121], veamos seguidamente su aplicación en el contexto de la lucha contra el terrorismo global donde se enmarca la creciente utilización de aparatos aéreos no tripulados.

2.- LOS DRONES COMO FACTOR EN LA SEGURIDAD MILITAR

En opinión del Instituto Internacional de Estudios Estratégicos[122], asistimos a una proliferación a escala global de la tecnología drone, en donde se calcula que más de setenta Estados cuentan con drones para ser utilizados en labores de seguridad o en operaciones militares, e incluso hay evidencias de que algunos grupos armados de carácter no estatal también han accedido a este tipo de artefactos, en donde según algunos informes[123], en el año 2006 Irán empezó a proporcionar drones armados a Hizbolá. En octubre de 2012 Hizbolá asumió el lanzamiento de un dron de reconocimiento y de combate Shahed-129, adentrándose 25 millas en Israel, habiendo filmado el reactor nuclear de Dimona, antes de ser derribado.

Es por ello que se observa una creciente atención al fenómeno de los drones tanto por parte de los estados[124] y sus fuerzas armadas como por

---

[121] HEYNS, C., *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Doc. ONU A/68/382, 13 de septiembre de 2013, p. 4.
[122] *The Military Balance 2014*, London, The International Institute for Strategic Studies, 2014, pp. 13-18.
[123] *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston, Addendum, Study on Targeted Killings*, U.N. Doc. A/HRC/14/24/Add.6, par. 27 p. 9.
[124] En este contexto, España y otros siete estados europeos, han firmado una carta de intenciones

parte de los Ministerios de Defensa y de Interior, en atención no solo a los desarrollos propios para fines de seguridad, sino para el control de su uso en el espacio aéreo dadas las potencialidades que pueden desarrollarse con esta tecnología[125], siendo en este contexto de amenaza latente, donde la guerra contra el terrorismo se configura como un conflicto armado en el que no existen limitaciones ni espaciales ni temporales, y ni mucho menos tecnológicas, pues nos encontramos ante una guerra sin caducidad contra los terroristas, se encuentren donde se encuentren según Milena Sterio.[126]

Si hay un ejemplo claro de la directa utilización de RPAS en la lucha contra el terrorismo es el programa utilizado por EEUU que empezó a usar drones de reconocimiento en la Guerra de Vietnam, y también los utilizó con esa misma finalidad en la primera guerra del Golfo (1991) y en los conflictos desencadenados en la antigua Yugoslavia, y ya en la década de los noventa, para misiones dirigidas a la obtención de inteligencia, vigilancia y reconocimiento aéreo, desempeñados, por sus modelos Global Hawk, Predator, Searcher y Raven, estos dos últimos, disponibles por las FFAA de España. A partir del año 2000 EEUU desarrolla la tecnología necesaria para dar a los drones un uso diferente al de reconocimiento e inteligencia, esto es el servir a su vez como plataforma de lanzamiento de misiles, controlados a larga distancia, siendo actualmente, los RPAS más utilizados el MQ1 o Predator, y el MQ-9 o Reaper, habiendo apostando por su utilización generalizada aduciendo como principal argumento su extraordinaria efectividad, basada a su vez en la alta popularidad que continúan teniendo los drones entre la opinión pública norteamericana[127]

---

con la Agencia Europea de Defensa (AED) para elaborar un estudio sobre la producción conjunta de drones de altitud media y gran autonomía.

[125] En este sentido, el Parlamento Europeo "manifiesta su grave preocupación en relación con el empleo de drones armados fuera del marco jurídico internacional" e "insta a la UE a que desarrolle una respuesta política adecuada a nivel europeo y mundial que respete los derechos humanos y el Derecho humanitario internacional", 2014/2567(RSP).

[126] STERIO, M., "The United States' Use of Drones in the War on Terror: The (Il)legality of Targeted Killings Under International Law", *Case Western Reserve Journal of International Law*, Vol. 45, 2012, pag. 202.

[127] Según una encuesta por el Pew Research Center, en 2013, un 61% de la opinión pública norteamericana aprueba los ataques selectivos con drones, superado únicamente por Israel, con un 64% de apoyo, mientras que tan solo un 30% los desaprueba. Mientras que a nivel global la utilización de drones es un fenómeno crecientemente impopular, con tan solo cuatro países (Israel, Estados Unidos, Kenya y Sudáfrica) en los que los partidarios de los drones superan a los detractores.

que consideraba esta como una lógica actuación en su defensa y apoyando de modo generalizado la puesta en marcha de una política de ataques selectivos sobre terroristas situados fuera del territorio nacional[128], mediante el uso de aviones no tripulados en zonas de conflicto como Afganistán e Irak, y llevadas a cabo por las Fuerzas Armadas estadounidenses, en respuesta a su derecho al ejercicio de la legítima defensa, reconocido por Consejo de Seguridad[129], tras los atentados del 11 de septiembre.

Aunque en palabras del Asesor jurídico del Departamento de Estado, "todas las operaciones selectivas de Estados Unidos, incluyendo operaciones letales llevadas a cabo, cumplen el derecho aplicable, incluido el derecho humanitario[130], mientras que por el contrario la campaña mediante drones sobre terroristas y líderes insurgentes que luchan contra

---

Mientras que en España se concluyó que había un 21% de la población a favor de su uso mientras que un 76% de los encuestados desaprobaban su utilización. Véase al respecto PEW RESEARCH CENTER, *Report questions drone use, widely unpopular globally, but not in the U.S.*, Washington, D.C., October 23, 2013, en *http://www.pewresearch.org/fact-tank/2013/10/23/report-questions-drone-use-widely-unpopular-globally-but-not-in-the-u-s/*

[128] UNITED STATES DEPARTMENT OF DEFENCE: U.S. *unmanned systems integrated roadmap (fiscal years 2009-2034)*, Washington DC, 2009, p. 2; El primer ataque fechado de Estados Unidos contra terroristas por medio de drones tuvo lugar en noviembre de 2002, en Yemen. En http://www. dtic.mil.

[129] De acuerdo con las normas de Derecho internacional, el *ius ad bellum*, es legítimo cuándo el uso de la fuerza en las relaciones internacionales debiéndose respetar unas normas en cuanto a los medios y métodos de combate, (el principio de proporcionalidad, entre la ventaja militar concreta esperada y los previsibles daños incidentales a civiles) y el de distinción entre objetivos civiles y militares), mientras que la prohibición del uso y amenaza de la fuerza contenida en el artículo 2.4 de la Carta admite dos excepciones: el ejercicio del "derecho inherente de legítima defensa individual y colectiva" en caso de ataque armado, reconocido en el artículo 51 de la Carta y también en normas de derecho consuetudinario, o la posible autorización del uso de la fuerza por parte del Consejo de Seguridad en el marco del Capítulo VII de la Carta. Siendo menester aquí incluir la decisión de La Corte Internacional de Justicia al señalar a este respecto que los Estados no deben usar armas que sean incapaces de distinguir objetivos civiles de militares, subrayando a su vez que para que un determinado tipo de armamento sea indiscutidamente contrario al Derecho Internacional Humanitario, necesariamente debe estar prohibido por medio de un Tratado internacional, según el artículo 8.2.b del Estatuto de Roma sobre la Corte Penal Internacional. http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95 ,

[130] El 21 de noviembre de 2012, se aprobaba por los EE. UU la Directiva 3000.00948 para, establecer "la política del Departamento de Estado y asignar responsabilidades para el desarrollo de las funciones autónomas y semiautónomas en los sistemas de armamento […] establecer parámetros para minimizar la probabilidad y consecuencias de los fallos y con el cuidado adecuado […] de acuerdo con el derecho de la guerra [y] los tratados aplicables […]En http://www.dtic.mil/whs/directives/corres/pdf/300009p. pdf)

las tropas de la coalición en Afganistán, pero refugiados en Pakistán es competencia de la CIA y no del Ejército estadounidense, respondiendo al hecho de que al no existir un conflicto armado entre Estados Unidos y Pakistán, es necesario restringir la presencia de miembros de las fuerzas armadas estadounidenses en territorio paquistaní, contando con la asistencia de contratistas de seguridad privada ejerciendo tareas de fuerzas de operaciones especiales.

La indudable capacidad de los RPAS estadounidenses basan su eficacia en los avances logrados en su perfeccionamiento, habiendo alcanzado los nuevos drones una enorme autonomía[131]que ha logrado una notable precisión adquirida en tareas de vigilancia durante largos períodos de tiempo, tanto en tareas de reconocimiento e inteligencia, como en la observación de personas sospechosas de llevar a cabo acciones terroristas, habiendo sido utilizado con asiduidad, quizás en menor medida durante la administración Bush y decididamente bajo la administración Obama[132], donde se observa una importante escalada en el número de servicios ejecutados en Afganistán, Somalia, Yemen, y Pakistán, por equipos de RPAS con y sin armamento[133].

El 23 de mayo de 2013, (con posterioridad al atentado de Boston) el Presidente Obama ofrecía un discurso en la Universidad de la Defensa Nacional, donde sentenció que Estados Unidos seguirá luchando contra Al Qaeda: "Debemos definir nuestros esfuerzos no como una ilimitada 'guerra global contra el terror', sino más bien como una serie de esfuerzos persistentes para desmantelar redes específicas de extremistas violentos que amenazan a América", mencionando entre sus frentes Afganistán, Pakistán, Yemen, Somalia, y extendiéndolo incluso a Malí y reiterando que

---

[131] LEWIS, M.W., "Drones and the Boundaries of the Battlefield", *Texas International Law Journal*, Vol. 47, Issue 2, 2012. Los drones han evolucionado su cada vez más larga duración de sobrevuelo, llegando a las 30 horas con el Predator B y a las 20 horas con el Predator C, esto es más de diez veces la autonomía de vuelo de los aviones tripulados, convirtiendo a los drones en un arma especialmente diseñada para labores de vigilancia y de ataque en operaciones antiterroristas.

[132]. Remarks by the President at the National Defense University, pp. 1-5, p. 2

[133] Véase "*Covert Drone War*", en *https://www.thebureauinvestigates.com/2015/09/02/monthly-drone-report-august-2015-32-us-strikes-hit-afghanistan-alone/* Donde según sus datos, desde el año 2004 todavía en administración Bush (Obama tomo el relevo en 2009) hasta el 3 de septiembre del 2015 se han utilizado drones en Afganistán en 43 ocasiones, en Somalia en 19 ocasiones, en Yemen 125 ocasiones, y en Pakistán 420 ocasiones

entre las posibilidades de iniciar "operaciones militares especiales", "ataques aéreos convencionales o con misiles" o la "invasión de territorios" la que resulta menos costosa y más precisa consiste en recurrir al ataque con drones armados. Ataques estos que considera ajustados a la legalidad internacional por llevarse a cabo en el contexto de una guerra en legítima defensa de los Estados Unidos contra Al Qaeda.

Aunque el argumento de la efectividad de los drones para el desarrollo de las hostilidades en el marco de un conflicto armado está ampliamente reconocida por los estados, en favor de la lucha contra el terrorismo, en los teatros actuales analizados, se debe reconocer, que el uso de drones plantea también la inevitable causación de daños a población civil[134], sobre todo en los contextos que hemos apuntado de Afganistán, Pakistán, Yemen o Somalia, donde los yihadistas como parte de su estrategia de ocultación, se entremezclan con la población civil, dificultando la plena efectividad[135] y poniendo en duda la decisión por parte de cualquier mando para ordenar el ataque sin previamente no haber estado basado en información precisa y fiable recogida por los servicios de inteligencia sobre el terreno[136], y que por ejemplo en los casos citados, se reconoce la existencia

[134]Según ttps://www.thebureauinvestigates.com/2015/09/02/monthly-drone-report-august-2015-32-us-strikes-hit-afghanistan-alone/ en Afganistán se contabilizan más de 40 bajas civiles, mientras que en Somalia superan los 100 civiles que perdieron la vida durante los ataques, aumentándose las cifras en Yemen hasta las aproximadamente 700 bajas civiles, mientras que en Pakistán ya se acerca a los 4000 los civiles muertos como consecuencia del ataque dron.

[135] El radio de acción de la explosión de un misil lanzado desde un drone, puede llegar hasta veinte metros, lo que puede hacer que las consecuencias del impacto se extiendan más allá del objetivo identificado, con el riesgo de que el manejo de los drones para ataques selectivos se acabe convirtiendo en una especie de juego virtual**.**

[136] Véase ANDERSON, D.E., "Drones and the Ethics of War", *Religion & Ethics NewsWeekly*, 14 May 2010. CLARKE, B.; ROUFFAER, C. and SÉNÉCHAUD, F., "Beyond the Call of Duty: why shouldn't video game players face the same dilemmas as real soldiers?", *International Review of the Red Cross*, Vol. 94, núm. 886, 2012. El uso de drones puede provocar una disociación física por una decisión con consecuencias fatales que se toma desde un lugar que se encuentra a miles de kilómetros de la realidad sobre el terreno, pudiendo conducir a una "mayor propensión a matar" en *http://www.pbs.org/wnet/religionandethics/2010/05/14/drones-and-the-ethics-of-war/6290/*. En contra algunos autores aseguran que la distancia física, la ausencia de stress y de cualquier tipo de peligro con la que se toman las decisiones a miles de kilómetros del campo de batalla pueden permitir decisiones mucho más racionales y consistentes con los principios básicos del DIH y del DIDH que cuando esas decisiones se toman desde un avión de combate. Véase McCLOSKEY, M., "The War Room: Daily Transition between Battle, Home Takes aToll on Drone Operators", *Stars and Stripes*, 27 October 2009, En *http://www.stripes.com/news/the-war-room-daily-transition-between-battle-home-takes-a-toll-on-drone-operators-1.95949*.

de fallos y lagunas que exigen extremar precauciones[137], y aunque es incuestionable la creciente utilización de los drones como una estrategia exitosa en la lucha contra el terrorismo, también es posible que se conviertan en la norma, "desplazando otras alternativas más respetuosas con la población civil"[138], en este sentido, diversas asociaciones de la sociedad civil se han movilizado para tratar de establecer controles sobre el fenómeno Drone, tales como la *ICRAC* (International Committe for Robot Arms Control)[139] para reflexionar sobre estas armas.

A su vez, Ben Emmerson, Relator Especial sobre contraterrorismo y derechos humanos, investigo en 2013 el lanzamiento de drones sobre civiles en varios Estados y, en agosto de 2013, el Secretario General de la Organización pedía un control de su uso, a la luz del Derecho Internacional. En febrero de 2014 el Parlamento Europeo aprobó, por una mayoría de 534 a 49, una resolución condenando el uso de los drones armados más allá del marco legal internacional y pidiendo a la UE una política sobre drones y armas autónomas, al no existir a nivel europeo una política definida sobre este respeto[140].

Con respecto a la política española al respecto[141], el Ministerio de Defensa ha apostado por aumentar la dotación de drones de que dispone, incluso la de la posibilidad de armar su modelo Atlante, que entre otros ya se utilizó en Afganistán con funciones de observación e inteligencia y protección de sus convoyes de vehículos militares. Hay que destacar que el

---

[137] Según el informe de la Universidad de Columbia y del Center for Civilians in Conflict, la precisión de los ataques con drones está condicionada por "fallos sistemáticos en la inteligencia sobre la que se basan dichos ataques, entre los que destacan las limitaciones técnicas de la propia video-vigilancia, la comprensión cultural del lugar y la fiabilidad de los informantes o gobiernos con los que se coopera". En Columbia law school human rights clinic and center for civilians in conflict, *The Civilian Impact of Drones: Unexamined Costs, Unanswered Questions*, New York, 2012.

[138] Columbia law school human rights clinic and center for civilians in conflict, *The Civilian Impact of Drones: Unexamined Costs, Unanswered Questions*, New York, 2012, p 3.

[139] Véase http://www.icrac.net

[140] Véase para un mayor entendimiento de la política UE: GUERRERO LEBRÓN, M. J., CUERNO REJADO, C., MÁRQUEZ LOBILLO, P., "Aeronaves no tripuladas: Estado de la legislación para realizar su integración en el espacio aéreo no segregado", *Revista de Derecho del Transporte*, núm. 12, 2013,

[141] El uso militar de los drones se contiene básicamente en la Orden PRE/1366/2010, de 20 de mayo, por la que se modifica el Reglamento de la Circulación Aérea Operativa, Real Decreto 1489/1994, de 1 de julio.

ejército español todavía no dispone de drones de Clase III (según OTAN, de más de 600 kg). Resta observar las implicaciones que añadirá la reciente Directiva (UE) 2016/970 de la Comisión de 27 de mayo de 2016, por la que se modifica la Directiva 2009/43/CE del Parlamento Europeo y del Consejo en lo que se refiere a la lista de productos relacionados con la defensa a efectos del EEE, en cuanto refiere en su articulado a los Drone como "Aeronaves", "vehículos más ligeros que el aire", "vehículos aéreos no tripulados", "UAVs", motores de aviación y equipo para "aeronaves", equipos asociados, y componentes, según se indica la nueva directiva, diseñados especialmente o modificados para uso militar.

En lo que respecta al uso de drones frente al terrorismo ha quedado patente que no se deben de desplazar las tácticas y estrategias de inteligencia habituales, dado que el fenómeno terrorista está extendido fuera de los teatros que hemos observado, y en donde de modo general la utilización de drones se antoja antagónica a la descripción que hemos detallado, direccionando si cabe su utilización a estrategias de inteligencia, observación y control de movimientos así como a otros usos como el control fronterizo, la seguridad y vigilancia por parte de las Fuerzas y Cuerpos de Seguridad, la gestión de los recursos naturales, la gestión de la calidad del aire o la supervisión e inspección de infraestructuras críticas.

3.- EL USO DE DRONES COMO FACTOR DE SEGURIDAD: ESTUDIO DE CASO EN APLICACIÓN COMO VIDEOVIGILANCIA EN LAS INFRAESTRUCTURAS CRÍTICAS

El interés por los drones como factor de seguridad[142] se centra principalmente en su posible utilización como elemento auxiliar o extensión

[142] Beneficios de los drones para la Seguridad según ESYS a través de su informe anual 2016 "La videovigilancia en la seguridad: Análisis y recomendaciones para su actualización legal"

a) La utilización de cámaras de televisión incorporadas a los drones en funciones de Videovigilancia no es nueva y se reconocen pruebas tendentes a su adaptación de acuerdo al momento social-legal y tecnológico, sin embargo, en nuestro país las empresas aún no lo han aplicado en el contexto de Seguridad Privada.

b) Se considera de gran estima a los drones para la Seguridad de sus empresas por su potencialidad y coinciden en que debieran permitirse, si bien, bajo el ordenamiento legal y la regulación de AESA.

de los (CCTV) y Videovigilancia, aplicada a funciones de Seguridad, analizando la disposición de cámaras de Televisión en drones cuyas imágenes grabadas, o trasmitidas en tiempo real, sean de utilidad en funciones de Seguridad tales como:

- Vigilancia de perímetros.
- Comprobación rápida de alarmas o incidentes.
- Rondas de vigilancia etc
- Vigilancia de áreas sensibles de difícil o peligroso acceso.

Uno de los campos donde ha demostrado su eficiencia en la videovigilancia de las infraestructuras críticas por múltiples riesgos[143], ya no solo naturales sino los propios deliberados mediante actos terroristas o mediante ciberataques, dado que actualmente resultan trascendentales para el normal funcionamiento de un estado. Consideramos que los RPAS son susceptibles de ocupar un importante lugar en la cadena de seguridad nacional[144], siendo indudable el factor que acompañan una utilización policial con fines de seguridad y vigilancia mediante los sofisticados sistemas integrados en los drones no necesariamente con la intención de sustituir otros factores de seguridad como los análogos mediante CCTV dado que las posibilidades del uso de drones mediante la toma de imágenes está sobradamente demostrado que aventaja cualquier concepción física de "vigilancia terrestre", dado que para llevar a cabo sus funciones de

c) Los drones se consideran de gran utilidad ante los nuevos retos en la protección de Infraestructuras Críticas y bienes singulares, provocados por la nueva tipología del agresor, sus nuevas herramientas y capacidades de actuación.

d) Se consideran muy útiles en vigilancia de grandes perímetros, rondas exteriores y en zonas poco accesibles.

Disponible en http://www.fundacionesys.com/es/documentos/la-videovigilancia-en-la-seguridad-analisis-y-recomendaciones-para-su-actualizacion-legal

[143] Múltiples riesgos entre los que se encuentran los ataques mediante drones, por lo que es menester adaptarse a la nueva arma tanto de ataque como de defensa. Francia investiga el vuelo ilegal de drones sobre siete centrales nucleares http://blogs.wsj.com/cio/2015/01/05/france-seeks-tech-to-stop-drone-flights-over-nuclear-plants/

[144] Un RPAS ligero es una solución competitiva que se puede integrar con otros sistemas y adaptar sus usos entre otros al control de fronteras, reconocimiento del terreno en catástrofes naturales, detección de contrabando en alta mar, supervisión de redes de transporte y vigilancia de infraestructuras críticas.

observación, supervisión y vigilancia, todos los RPAS comerciales o policiales van equipados con cámaras que producen imágenes extremadamente nítidas y, en algunos casos, también pueden contar con equipos de grabación de sonido, cámaras de infrarrojos y detectores térmicos así como herramientas de reconocimiento facial y biométrico en tiempo real, lo que hace posible monitorizar y todo esto, desde una posición estratégicamente aventajada, dada la capacidad del drone de mantenerse estático en una misma posición (*hovering)*[145]

Así pues, los elementos esenciales de cualquier sistema de seguridad deberían de tener en consideración la utilización de drones por parte de los sectores público y privado especialmente cuando se trata de la videovigilancia de los sectores estratégicos, utilizando estos dispositivos para asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como para prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública, en donde se estaría cumpliendo estrictamente en igualdad de condiciones a las descritas en la Ley Orgánica 4/1997, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos en labores preventivas de vigilancia y control[146] del orden público o la propia Ley 5/2014, de 4 de abril, de Seguridad Privada, en donde en su art 42.1 Servicios de videovigilancia, menciona que "Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o *móviles*[147], capaces de captar

[145] Los drones más idóneos para aplicaciones de seguridad en infraestructuras críticas son los helicópteros y quadrotors, aunque en algunas infraestructuras, como por ejemplo la vigilancia de un tendido férreo, podría ser más interesante el empleo de otro tipo de UAV; pero para la mayor parte de las instalaciones esenciales, los quadrotors y helicópteros serán suficiente.

[146] La policía de los Estados Unidos ha sido oficialmente la primera en utilizar drones armados desde el 8 de agosto 2015. http://www.thedailybeast.com/articles/2015/08/26/first-state-legalizes-armed-drones-for-cops-thanks-to-a-lobbyist.html Para mayor información sobre este tema en FINN, R.L., WRIGHT, D., Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. ELSEVIER. 2012.

[147] Cursiva nuestra, para determinar el encaje y procedencia que se acomoda al fenómeno Drone al poder considerar a este dispositivo como un servicio de videovigilancia móvil. También existe otra posible asimilación normativa respecto a la asimilación de los drones como servicio de videovigilancia móvil cuando se matiza que "Para la utilización puntual o esporádica de *cámaras móviles* en vías en las que no está autorizado el uso de cámaras fijas, su uso deberá aprobarse por la máxima autoridad provincial de las Fuerzas y Cuerpos de Seguridad. Esta resolución se pondrá en conocimiento de la Comisión antes mencionada en el plazo máximo de 72 horas.

y grabar imágenes y sonidos, *incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas*".

En el caso que sea procedente la utilización de drones para monitorizar aquellos espacios que se han identificados como objetivos por razones de seguridad o cualquier otro motivo con interés legítimo, (interés que presenta en este sentido las infraestructuras críticas generalmente), se debe erradicar o minimizar la captación de imágenes de zonas privadas no comprendidas dentro del área de actuación y, de manera especial, los interiores de edificios o zonas residenciales fuera del espacio monitorizado, cuestión esta que nos parece salvable dada la capacidad de programación que sustentan los drones actuales capaces de discriminar la información dependiendo de los parámetros de programación establecidos, circunscribiéndose incluso a pesar de sus altas capacidades en cuanto a distancias de observación, a la que previamente fuera delimitada mediante vallas u otro tipo de cerramiento en donde a su vez, deberá indicarse mediante el uso de carteles o señales, la existencia de "Drone en operación de videovigilancia".

No obstante debemos también considerar en este ámbito, la necesaria distinción entre los usos de drones por parte de las Fuerzas y Cuerpos de Seguridad en sus ámbitos de actuación y fundamentalmente los dedicados a la persecución de los delitos y/o la prevención de los mismo de cualquier otros usos civiles y comerciales que puedan llevar a cabo empresas privadas y organismos públicos, dado que en el caso de la posible utilización de estos sistemas por parte de las empresas de seguridad privada, entrarían en el supuesto que se le atribuye a las propias Fuerzas y Cuerpos de Seguridad al actuar la seguridad privada bajo los parámetros de actuación determinados previamente por la dirección general de policía.

En este sentido y siguiendo el ejemplo de una dispositivo de vigilancia mediante drones en una infraestructura crítica, pues no debemos ser ajenos a las capacidades que dispone la tecnología actual al dotar de videovigilancia mediante Drone a las infraestructuras críticas[148].,

[148] Repsol despliega drones para vigilar infraestructuras críticas Serán utilizados para la inspección de plataformas petrolíferas en el mar, cartografiar posibles yacimientos y detectar fugas Los drones llegan también a la industria del petróleo. Repsol va a incorporarlos a su tecnología para obtener

necesariamente estas deberán contar entre su personal con los operarios necesarios que dirigirán, mantengan y controlen el Drone, estando debidamente acreditados por las autoridades competentes, e igualmente, deberán nombrar una figura que se encargue de la protección de datos, que se encargará de supervisar la correcta utilización de los datos personales obtenidos y mantener contacto con los entes nacionales e internaciones de protección de datos al objeto de someterse a sus regulaciones.

Describimos según Canosa Rodríguez [149] las principales razones que redundan particularmente en la procedencia del uso de drones en la videovigilancia de las infraestructuras críticas.

- Reducción de riesgos para los vigilantes: Este es la ventaja más inmediata de la utilización de robots para las tareas de vigilancia de una instalación. Concentrando la intervención humana en uno o varios operadores, en función de la complejidad de la instalación.
- Intensificación de la vigilancia: Un sistema robótico permite la realización de un mayor número de rondas de vigilancia y que estas sean más exhaustiva eliminando sesgos humanos.
- Mejora en la capacidad de percepción de datos: Los sensores utilizados en los sistemas robóticos son en su mayor parte más precisos que los sistemas sensoriales de los vigilantes humanos. Además se puede equipar estos robots con sensores que añaden información que no podrían obtener vigilantes humanos, como por ejemplo información de temperatura obtenida con cámaras termográficas.
- Movilidad ampliada independientemente de los errores topográficos: Un sistema basado en sensores estáticos centrará la vigilancia en una determinada zona que puede ser más o

imágenes en alta resolución y evaluar el estado de estructuras que superan los 100 metros de altura http://www.elconfidencialdigital.com/dinero/Repsol-despliega-vigilar-infraestructuras criticas_0_2540745904.html

[149] RODRIGUEZ CANOSA, G,R; BARRIENTOS CRUZ, A; CERRO GINER, J., Caracterización de las infraestructuras críticas de exteriores y su influencia sobre sistemas de vigilancia robóticos. 2011. págs. 3 y 35.

menos amplia. Sin embargo, con un sistema de robots es posible centrar la vigilancia en determinadas zonas que podrían no estar cubiertos por lo sensores. Además el uso de robots también posibilita ampliar la zona vigilada en determinados y motivados instantes.

- Tareas de inspección: Un sistema robótico de vigilancia puede usarse también para tareas de inspección, asignando diferentes prioridades a cada tipo de tarea, aumentando así la efectividad del sistema y contribuyendo a mejorar la seguridad de la instalación.

Según el citado autor, las características técnicas que deberían cumplir los drones que participen en la seguridad, serán las definidas por la OTAN como de primer nivel y básicamente con dimensiones máximas de entre 1 y 2 metros y con pesos entre 3 y 50 kg. La autonomía necesaria dependerá de diversos factores, pero básicamente con una autonomía de aproximadamente 2h y velocidades máximas de 50 km/h y contar con la capacidad de mantenerse estático en una misma posición (*hovering).*

4.- LOS DRONES DE USO CIVIL

Generalmente la principal preocupación que subyacía en la anterior década sobre el uso y regulación de los Drone, radicaba en que se pudiera conseguir un alto nivel de seguridad en su uso que fuera equiparable al que ofrecen las aeronaves tripuladas, mientras que en la actualidad, como refiere Pauner Chulvi, se ha dado paso a un perceptible movimiento normativo[150] centrado ya no en las capacidades o características de los Drone, derivando este énfasis legista a un creciente interés en la defensa de los derechos de los ciudadanos, exigiendo la incorporación de garantías relativas a la protección de la vida privada y de los datos personales, que podrían no verse garantizados en un estado de derecho, dadas las altas

[150] PAUNER CHULVI, C, "El uso emergente de drones civiles en España. Estatuto jurídico e impacto en el derecho a la protección de datos" *Revista de Derecho Político* UNED, N.º 95, enero-abril 2016, p. 87

capacidades de estos aparatos y lo avanzado de su tecnología, donde le paso más importante para su desarrollo normativo bajo estas premisas, bajo el paraguas de la Unión, se residencia en la normativa referenciada, dado con la adopción de la Resolución del Parlamento Europeo, de 29 de octubre de 2015, sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil. Veremos con posterioridad un tratamiento directo sobre este factor respecto a la posible causación de daños en la esfera personal de las personas o vulneraciones de la ley de protección de datos durante el uso y navegación de los Drone.

En este epígrafe sobre los Drone de uso civil es necesario previamente categorizar y describir que entendemos por uso civil de drones, máxime habiendo visto con anterioridad múltiples usos para la seguridad o con fines militares. En España atendiendo al estado actual de la regulación, sin abundar nuevamente en su carácter transitorio, podemos distribuir los usos civiles de los drones como de uso profesional, y de uso recreativo. Los drones de uso Profesional[151] dentro de este marco civil, según la Ley 18/2014 viene determinados por una serie de requisitos de explotación, en su utilización básicamente con fines científicos y técnicos, tales como: actividades de investigación y desarrollo; tratamientos aéreos, pesticidas y otros tratamientos que implican la difusión de sustancias en el suelo o la atmósfera, incluidas las actividades de lucha contra el fuego; observación y actividades de vigilancia aérea, incluyendo la filmación y el seguimiento de los incendios forestales; publicidad, emisiones aéreas de radio y televisión y de emergencia, operaciones de búsqueda y rescate, así como otras obras especiales. donde la ley describe múltiples requisitos de utilización que básicamente deberán realizarse durante el día y en condiciones meteorológicas visuales, en espacio aéreo no controlado, dentro del alcance

[151] Ley 18/2014 art 50.3 y 4. Podrán realizarse actividades aéreas de trabajos técnicos o científicos por aeronaves civiles pilotadas por control remoto, de día y en condiciones meteorológicas visuales: Vuelos de prueba realizados por fabricantes u organizaciones dedicadas al mantenimiento, vuelos de demostración no abiertos al público dirigidos a grupos cerrados de asistentes a un determinado evento o de clientes potenciales de un fabricante u operador , Vuelos para programas de investigación, nacionales o europeos, en los que se trate de demostrar la viabilidad de realizar determinada actividad con aeronaves civiles pilotadas por control remoto, vuelos de desarrollo de nuevos productos o para demostrar la seguridad de las operaciones específicas de trabajos técnicos o científicos. Vuelos de I+D realizados por fabricantes etc.

visual del piloto, o, en otro caso, en una zona del espacio aéreo segregada al efecto y siempre en zonas fuera de aglomeraciones de edificios en ciudades, pueblos o lugares habitados o de reuniones de personas al aire libre y a una altura máxima de 120 metros, acotadas al espacio aéreo no controlado estableciendo zonas y pasillos aéreos de uso reservado y exclusivo para los drones.[152]

Es preciso matizar que la ley 18/2014, se muestra extremadamente garantista, cuando especifica que aun estableciéndose por el operador del uso comercial o técnico profesional de las distintas obligaciones descritas en el art 50, «no exime al operador, que es, en todo caso, el responsable de la aeronave y de la operación, del cumplimiento del resto de la normativa aplicable, en particular en relación con el uso del espectro radioeléctrico, *la protección de datos o la toma de imágenes aéreas,* ni de su responsabilidad por los daños causados por la operación o la aeronave» (artículo 50.1). Concretamente, la protección de la intimidad y la protección de los datos de carácter personal obliga al operador a adoptar las medidas necesarias para garantizar el cumplimiento de lo dispuesto en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD).

Respecto al uso recreativo o lúdico presenta múltiples dificultades poder acotarlo pues no se rige por la LNA[153], observando a través de la legislación su aplicación respecto a demostraciones aéreas que no se encuadren en otras categorías por tamaño, peso y altitud, distintas actividades deportivas, recreativas o de competición. Cabe matizar igualmente que aunque los Drone sean empleados con fines deportivos o de ocio[154], deben someterse igualmente a la observación de las leyes aeronáuticas vigentes.

---

[152] La OACI divide al espacio aéreo en siete partes, nombradas con una letra de la A a la G. La clase A es el sector con el nivel más alto de control, mientras que la clase G refiere al espacio aéreo no controlado. Cada calificación indica las normas operativas, el equipamiento mínimo y los requisitos que los pilotos deben respetar para poder volar.

[153] Ley 48/1960, de 21 de julio, de Navegación Aérea. art 150.2. excluye de su aplicación la operación de aeronaves civiles pilotadas por control remoto al describirlo del siguiente modo "excepto las que sean utilizadas exclusivamente con fines recreativos o deportivos"

[154] El borrador no oficial de Real Decreto por sancionar, si parece que describirá profusamente el

Si entendemos como parece ser que se definirá a los Drone de uso recreativo como "aeromodelos radio-controlados", debemos especificar que los aeromodelos también se someten a regulación y en el caso de España, esta se encuentra referenciada en la normativa de la Real Federación Aeronáutica de España[155]y suponiéndose que deberá considerarse como vuelo radio-controlado, por lo que igualmente debe asegurarse la seguridad de los mismos mediante el cumplimiento de los requisitos aplicables para la realización y autorización de una demostración aérea civil según la normativa, sometiéndose también no solo a esta normativa específica pues además deberá acomodarse a cada regulación de las distintas comunidades autónomas debiendo atender el operador de un Drone para uso lúdico, no solo a la legislación nacional sino también a las posibles normativas provinciales y ordenanzas municipales, además y como punto a incluir en el siguiente epígrafe, el operador de un Drone para uso civil, con fines de recreo y lúdicos, observar lo dispuesto en la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y en la Ley Orgánica de Protección de Datos, si el Drone está dotado del ingenio necesario para filmar y captar imágenes.

5.- LOS DRONES Y SU IMPACTO EN LA LEGISLACIÓN DE PROTECCIÓN DE DATOS Y LAS POSIBLES COLISIONES CON LA PROTECCIÓN DE DERECHOS DE LA ESFERA PERSONAL

La legislación española respecto a las garantías y obligaciones descritas en la ley Orgánica de Protección de Datos (LOPD), actualmente[156],

uso de los Drone con fines de ocio a los que denomina como "aeromodelos radio-controlados", y que básicamente se resumen en que el vuelo deberá realizarse en condiciones diurnas y en condiciones meteorológicas de vuelo visual, dentro del alcance visual del piloto, en zonas autorizadas fuera de áreas pobladas, en espacio aéreo no controlado, manteniendo una distancia adecuada a los obstáculos y en zonas fuera de aglomeraciones de edificios en ciudades, pueblos o lugares habitados o sobre una reunión de personas al aire libre.

[155] Entre otros, *Real Decreto 1919/2009, de 11 de diciembre, por el que se regula la seguridad aeronáutica en las demostraciones aéreas civiles.*

[156] La legislación española respecto a las garantías y obligaciones descritas en la ley Orgánica de Protección de Datos (LOPD) fue dictada como trasposición y armonización de la Directiva 95/46/CE. El 15 de diciembre de 2015, el Consejo, el Parlamento y la Comisión de la Unión Europea

no contiene alusiones directas a la figura de los drones, pero es muy clarificador el enunciado que subyace sobre el tratamiento de la imagen y esta imagen definida como dato cuando en su art 3.a, define "A los efectos de la presente Ley Orgánica" como dato personal, que este se entenderá por, "cualquier información concerniente a personas físicas identificadas o identificables", profusamente referida en el mismo sentido en el reglamento de desarrollo de la propia ley cuando en su art 5.1.f), respecto a los aludidos datos de carácter personal, refiriéndolos como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables", deduciéndose de esta interpretación, que las imágenes captadas por un Drone, coincide con el tipo descrito pues la capacidad de obtener imágenes, incluso imágenes por infrarrojos y también sonidos, elementos todos estos descritos en la LOPD como datos personales, resultando de esta colisión, que un Drone, deberá respetar igualmente los principios y garantías establecidos en la citada ley, donde la afectación sobre los derechos salvaguardados por la citada ley, incidirá en proporción al uso que se administre al Drone, pues no será pertinente observar problemas de salvaguarda de la intimidad cuando el Drone acometa funciones de vigilancia de cultivos, mareas, bancos de pesca, control de incendios, etc, también deberán ser observados los propios que la ley describe como "ejercicio de actividades exclusivamente personales o domesticas" según refiere al art 2.2ª de la LOPD, en las que podría encuadrarse en actividades de la vida privada familiar, entre otras, grabarse o fotografiarse a sí mismos practicando deporte, grabaciones o fotografías en una celebración familiar, etc, cuestiones estas directamente relacionada con las funciones y fines de la mayoría de drones puestos en venta y al alcance del público que y que

alcanzaron un acuerdo sobre el texto final del futuro Reglamento General de Protección de Datos el 27 de abril de 2016 y que tiene como objetivo la actualización de las disposiciones contenidas en la Directiva 95/46/CE. A través del nuevo Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, 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 derogara en mayo del 2018 la Directiva 95/46/CE (Reglamento general de protección de datos), e incluirá una Directiva sobre protección de datos en el ámbito policial que derogara la Decisión Marco 2008/977/JAI del Consejo, haciendo un especial énfasis como refiere la nueva normativa "en particular, las que implican el uso de nuevas tecnologías" por lo que influirá en la actual LOPD que deberá acomodarse a la futura Directiva desde el 25 de mayo de 2018.

podría sustentar un uso licito, dentro de los parámetros descritos, no debiéndose en principio, verse sometidos a la propia LOPD, aunque deban someterse a las obligaciones establecidas en la ley, y en las distintas leyes que especifiquen el uso de Drone, estatales, autonómicas y municipales, respecto al uso del espacio aéreo.

La utilización de drones por los particulares, con otros fines que no encajen en los propios descritos con encaje en el art 2.2 citado, siempre y cuando el Drone este equipado con tecnología de videograbación, deberá someterse a las obligaciones establecidas en la ley, y en el mismo sentido descrito anteriormente, las distintas leyes que especifiquen el uso de Drone, estatales, autonómicas y municipales. Recordemos que nuestra LOPD es una trasposición armonizadora de la Directiva 95/46/CE , que en el 25 de mayo de 2018, será sustituida por el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[157], 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), pertinente a efectos del EEE, donde este futuro Reglamento 2016/679 de Protección de Datos tiene como objetivo "dar más control a los ciudadanos sobre su información privada"[158], por lo que las nuevas reglas incluyen la necesidad

[157] Con esta nueva norma se acabaron los conocidos en España como derecho ARCO (Acceso, Rectificación, Cancelación y Oposición) Capítulo III. Derechos del interesado; 1.ª Transparencia y modalidades (art. 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado); 2.ª Información y acceso a los datos personales (arts. 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado, a 15. Derecho de acceso del interesado); 3.ª Rectificación y supresión (arts. 16. Derecho de rectificación, a 20. Derecho a la portabilidad de los datos --incluyendo el importante art. 17. Derecho de supresión («el derecho al olvido»)--; 4.ª Derecho de oposición y decisiones individuales automatizadas (arts. 21. Derecho de oposición, y 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles) y 5.ª Limitaciones (art. 23. Limitaciones).
http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679#document1

[158] Conforme al artículo 18.1 de la Constitución, el derecho al honor y a la intimidad personal y familiar, tiene el rango de fundamentales, y hasta tal punto aparecen realzados en el texto constitucional que el artículo 20.4, dispone que el respeto de tales derechos constituya un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales. El artículo 105 del mismo texto constitucional también determina que el acceso de los ciudadanos a los archivos y registros administrativos tendrá siempre en cuenta el derecho a la intimidad de las personas. Posteriormente, la Ley Orgánica la 1/1982, de 5 de mayo, de Protección del derecho al honor, a la intimidad personal y a la propia imagen, dice en su artículo 7.4 que se considerará intromisión ilegítima la revelación de datos privados de una persona conocidos

de un "consentimiento claro y afirmativo" de la persona concernida al tratamiento de sus datos personales, la "portabilidad" o el derecho a trasladar los datos a otro proveedor de servicios, el derecho a ser informado si los datos personales han sido pirateados, un lenguaje claro y comprensible sobre las cláusulas de privacidad, y la posibilidad de ejercer el mencionado derecho al "olvido", mediante la rectificación o supresión de datos personales en internet.

Especial tratamiento al objeto de este trabajo merece el empleo creciente de drones por las Fuerzas y Cuerpos de seguridad estatales, demostrándose su alta eficacia cuando tales equipos, dadas sus altas capacidades, pueden grabar a distancia, al estar diseñados, dispuestos y equipados con sensores biométricos para tareas de videovigilancia, especialmente útiles para el control de entre otros, de fronteras terrestres para el control de migraciones o los usos de control en zona marítima como el seguimiento de embarcaciones que presumiblemente estén realizando

a través de la actividad profesional. Por otro lado, en la Declaración Universal de Derechos Humanos, promulgada por la Asamblea General de Naciones Unidas el 10 de diciembre de 1948, se establece en su primer artículo que los seres humanos nacen libres e iguales en dignidad y derechos, y dotados como están de razón y conciencia, han de comportarse fraternalmente los unos con los. La proclamación de la dignidad de la persona y del mismo grado de dignidad en todas las personas, nos vale como presupuesto clave para entender que no hay razón posible de discriminación en este sentido. Por el mero hecho de ser persona todos tenemos la cualidad jurídica de la personalidad, y de ésta se deriva expresamente la dignidad personal. A su vez y de ahí se derivan una serie de derechos, de los que la persona es único titular. Del mismo modo, como consecuencia del artículo octavo de esta Declaración, se reconoce y auspicia el derecho efectivo a poder recurrir ante los tribunales nacionales cualquier atentado contra actos que violen los derechos fundamentales reconocidos en la Constitución. El artículo duodécimo señala que nadie será objeto de injerencias arbitrarias en la propia vida privada, en su familia, en su domicilio o su correspondencia, ni de ataques a su honra o reputación. Así, toda persona tiene derecho a la protección de la ley contra tales injerencias, o ataques. Se defienden aquí el derecho subjetivo a la intimidad y al honor y obliga a los Estados a defenderlos de los posibles ataques o injerencias. En muy similares términos se defienden estos derechos desde el Internacional de Derechos Civiles y Políticos, de 1966 y la Convención Europea para la salvaguarda de los derechos humanos y libertades fundamentales, de 1950. La función atribuida por el Ordenamiento Jurídico al derecho a la intimidad es la de proteger frente a posibles invasiones que pudieran producirse en aquel ámbito de la vida personal y familiar que la persona desee excluir del conocimiento ajeno e intromisiones de terceros en contra de su voluntad. A diferencia de lo anteriormente dicho, el derecho a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre el uso y destino dado a los mismos, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado. Esto significa que mientras que el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno y confiere el poder de resguardar su vida privada de una publicidad no querida, el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos

tareas ilícitas etc, en donde debemos deducir que el tratamiento de datos personales que pudieren verse comprometidos por el uso de las videograbaciones efectuadas por los Drone, deberán acomodarse y someterse a la disposición especifica del sector 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[159], que aunque no refiera explícitamente a los Drone, es de aplicación en este sentido, lo descrito en el art 5 de la citada ley, que autorizando la utilización de videocámaras móviles, y siempre atendiendo a la pertinencia de su uso, un "peligro concreto" para la seguridad ciudadana, deberá esta ser ajustada al principio de proporcionalidad en su doble versión de idoneidad y de intervención mínima, (la vigilancia indiscriminada[160], el tratamiento masivo de datos o la puesta en común de datos y perfiles) donde las imágenes y sonidos obtenidos accidentalmente, deberán ser destruidos inmediatamente por quien tenga la responsabilidad de su custodia, sabiendo que el plazo de cancelación de las grabaciones será de un mes, con la salvedad de las imágenes relacionadas con infracciones penales o administrativas graves,

[159] El Real Decreto 596/1999, de 16 de abril, de desarrollo de la citada ley, excluye su aplicación a las instalaciones fijas de videocámaras que realicen las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad en sus inmuebles, siempre que éstas se dediquen exclusivamente a garantizar la seguridad y protección interior o exterior de los mismos y a las unidades de Policía Judicial cuando, en el desempeño de funciones de policía judicial en sentido estricto, realicen captaciones de imágenes y sonidos mediante videocámaras que se regirán por la Ley de Enjuiciamiento Criminal y por su normativa específica. Por tanto, según cita PAUNER CHULVI, en estos casos resulta de plena aplicación lo dispuesto por la LOPD y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Citado en PAUNER CHULVI, C,"El uso emergente de drones civiles en España, … *Ob cit*, p. 96

[160] Es importante destacar la utilización de la técnica del *profiling* que consiste en un proceso de acumulación y análisis masivo de datos de carácter personal para la elaboración de bases de datos elaborando perfiles que se puedan utilizar para realizar valoraciones o tomar decisiones sobre los sujetos La elaboración de perfiles, ha sido utilizada para predecir patrones de comportamiento de riesgo en la población y tomar decisiones para atajar actividades delictivas o en la lucha antiterrorista, pero, esta técnica puede provocar discriminación mediante la identificación de las personas o grupos sociales para aplicarles un tratamiento desfavorable basado en suposiciones erróneas, recordemos que los Drone pueden estar equipados con tecnología de reconocimiento facial y biométrico que hace posible monitorizar y discriminar la toma de imágenes basándose en criterios biométricos. Para un mayor abundamiento sobre la cuestión véase el d*ocumento de asesoramiento sobre los elementos esenciales para una definición y regulación de la técnica de elaboración de perfiles en la Propuesta de Reglamento de Protección de Datos*, 13 de mayo de 2013.

con la correspondiente obligación de reserva por parte de los que tengan acceso a estas imágenes.

Se plantean dificultades en el uso por parte de las Fuerzas y Cuerpo de Seguridad del Estado, entre otras[161] el derecho a ser informado mediante la existencia de videovigilancia mediante Drone, y de difícil traslado a uso real de estos mecanismos por ejemplo durante una manifestación etc, donde por ejemplo propone, Elodi Villena, que sería factible para cumplir con la obligación informativa en estos casos, plantear por parte de las autoridades públicas a través de los medios de comunicación, la publicidad que anunciara que tal evento será "video-vigilado mediante Drone"[162], mientras que la utilización por el sector de la seguridad privada [163], por parte de las

[161] También resulta complejo el tratamiento de las imágenes obtenidas con fines de control de tráfico, dado que el tratamiento de imágenes y sonidos se les debe aplicar supletoriamente la LOPD

[162] ELODI VILLENA, M., «El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración», en *Congreso Derecho TICS - SICARM 2014*, Barcelona, 23-24 de octubre de 2014, pág. 6. Citado en CHULVI p 99

[163] La videovigilancia operada por el sector privado se describe en la Ley 5/2014, de 4 de abril, de Seguridad Privada en *Artículo 42 Servicios de videovigilancia*

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los

autoridades o por parte de las empresas de seguridad privada habilitadas en recintos abiertos o no al público o en la propia vía pública, etc además de merecer un capítulo aparte por la relevancia y por la dispersión de la normativa que en el caso de la seguridad privada, podría desvirtuarse dadas las múltiples utilidades que contempla, donde inicialmente este se asemeja al uso los sistemas de Circuito cerrado de televisión, la grabación y el tratamiento de datos mediante el uso de drones plantea colisiones con los principios de finalidad y proporcionalidad porque, a diferencia de los sistemas de vigilancia CCTV, los drones son aéreos, móviles, discretos y pueden ir equipados con sofisticadas tecnologías que permiten el almacenamiento masivo e indiscriminado de datos, pudiendo utilizarse esos datos para fines distintos, o por ejemplo dado el sometimiento del sector privado, podría este desvirtuarse y ser utilizado con otros fines tales como el empleo de Drones para vigilar a los trabajadores, su producción o sus interacciones entre estos de ámbito privado[164], desviando el uso inicialmente previsto por el Drone, contratado al proveedor del servicio.

6.- CONCLUSIONES

El empleo de aviones no tripulados ha generado una controversia notable, dado que actualmente, diversos estados han potenciado como instrumento letal para llevar a cabo las campañas de ataques selectivos contra miembros de grupos terroristas trasnacionales. Ante este panorama la opinión pública puede mantenerse reacia a vislumbrar las potencialidades que representa la labor de los drones y en este sentido según este artículo, la ingente labor de videovigilancia y control que

sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

A este respecto, debemos igualmente observar el Informe de la AEPD sobre Normativa aplicable a tratamientos de datos personales con fines de videovigilancia (Informe 0314/2009).

[164] Según el 36 RLOPD 44 se establece que los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, basada únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

podrían realizar los Drone en las infraestructuras críticas, no en vano existe una preocupación generalizada en los estados a la que no es ajena España, o Europa, por la protección de este tipo de instalaciones ante amenazas deliberadas y en particular las amenazas terroristas actuales. Creemos que con una fundamentación adecuada apoyada en un corpus legal y normativo consensuado, sería posible incluir a los drones como elemento de seguridad en las infraestructuras críticas para ejercer labores de vigilancia y control de la propia infraestructura, que redunden en la más alta protección posible ante cualquier amenaza y en particular la amenaza terrorista. Por otra parte, el uso de los Drone también ha evidenciado la necesidad de articular y armonizar normativas para la salvaguarda de los derechos de la esfera personal de los posibles ciudadanos captados. La protección de datos de carácter personal, tanto en el Ordenamiento Jurídico español como en el plano comparado, es un derecho fundamental de relativamente reciente aparición si se le compara con otros de larga tradición, como el honor o la libertad de expresión. No es de extrañar si se tiene en cuenta la relación lógica que éste mantiene con el desarrollo de la tecnología, especialmente la informática, y la necesidad de reaccionar frente a los riesgos que ésta puede representar para la libertad y la intimidad de los ciudadanos. La Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal, entronca con una rama fundamental de nuestro Derecho, como es la rama constitucional. Y esto se desprende, sin lugar a dudas, nada más comenzar a leer la misma puesto que en su artículo 1 se consagra el derecho al honor y a la intimidad personal y familiar, precepto que a todas luces entronca con el consagrado en el artículo 18 de nuestra Constitución. Estos derechos, no hacen más que consagrar dentro del marco de las libertades personales la expresión de un derecho global a la privacidad, que de una u otra manera coincide con el derecho a la intimidad entendido en sentido amplio, es decir, como derecho a la autodeterminación de la vida privada. El derecho a la privacidad comprende el reconocimiento de todos los derechos recogidos en el artículo 18 de nuestra Constitución. El principio de información que se describe en la LOPD exige que se deberá previamente, ser informados los interesados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter

personal, de la finalidad de su recogida y de los destinatarios de los mismos (artículo 5 LOPD). Cuestión esta que planteamos de compleja aplicación respecto al uso de drones con fines de videovigilancia por parte de las autoridades y del mismo modo la que los particulares pudieran captar, fuera del rango de acción de la contemplada como zona de su uso privado. Por este motivo es importante que la ciudadanía conozca las repercusiones que subyacen del empleo de las tecnologías drones, aplicadas a la seguridad y a la vigilancia, donde igualmente los operadores civiles de los Drone, deberán también conocer no solo las obligaciones normativas de su uso sino también, con mayor énfasis, las consecuencias y responsabilidades derivadas de sus actividades sobre los derechos a la protección de datos y la privacidad de la ciudadanía.

En este sentido, sea quien fuere el titular del Drone, la normativa le exige el cumplimiento del principio de información, debiendo ser publicado o publicitado, incluyendo la identidad del operador del dron o su representante, así como los derechos que asisten a los sujetos titulares, dado que reconoce la propia ley que si el ciudadano desconoce o no es consciente de la presencia de un Drone, este no podrá ejercer de manera adecuada los derechos que le asisten respecto al tratamiento de su imagen como dato personal, sin poder ejercer por tanto de manera concreta sus derechos ante el operador del Drone, en principio ante la legislación dispuesta a través de ARCO, y cuando entre la nueva trasposición del nuevo 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)

También la LOPD describe, que este consentimiento habrá de ser expreso y por escrito si los drones se emplean en espacios que, por su naturaleza o características, pueden comportar la captación de imágenes que pudieran revelar la ideología, afiliación sindical, la religión o las creencias de las personas afectadas, en donde a tenor de esta línea de trabajo, el Grupo Europeo en Ética de las Ciencias y las Nuevas Tecnologías, observa que las empresas privadas como las autoridades públicas, deberán

adoptar los principios de las PET en el desarrollo de las nuevas tecnologías de vigilancia y seguridad, implementadas entre otros en los mecanismos Drone, entendiendo el grupo europeo en Ética de las Ciencias y la Nuevas Tecnologías que «los valores europeos de dignidad, libertad y justicia deben tenerse en cuenta antes, durante y después del proceso de diseño, desarrollo y ejecución de esas tecnologías. Las tecnologías de protección de la intimidad deben incorporarse desde la fase inicial y no añadirse como un apéndice posteriormente»[165]. La carencia de una normativa concreta y explicita respecto a los usos de los Drone, y su incursión como elemento que entra en colisión con la naturaleza de distintos derechos de la esfera personal, deberá atenderse al marco legal existente en materia de protección de datos, puesto que los problemas que los drones plantean en relación con la protección de datos no son nuevos, puesto que la tecnología de la que se brinda, esto es la video imagen ya no representa ninguna novedad, pues tan solo representa una novedad y desafío al derecho, el vehículo que la porta y transporta y que basa esta novedad, en configurarse como una herramienta que dispone de una muy versátil movilidad, en un reducido tamaño, la posibilidad de resultar invisible o difícilmente detectable por el usuario de la vía pública, la posibilidad de disponer de criterios preinstalados de captación aleatoria de imágenes con fines de realizar perfiles y la accesibilidad a cualquier usuario para su adquisición[166].

7.- REFERENCIAS

ACED FÉLEZ, E., «Drones: una nueva era de la vigilancia y de la privacidad», *Seguritecnia*, núm. 403, 2013.

[165] Grupo Europeo de Ética de las Ciencias y las Nuevas Tecnologías, *Dictamen sobre Ética de las Tecnologías de la Seguridad y la Vigilancia*, cit., pág. 91.

[166] El Parlamento Europeo se suma a estas consideraciones solicitando a la Comisión que, en el desarrollo de drones, se incorporen garantías relativas a la protección de la vida privada y de los datos incluyendo entre los requisitos mínimos la obligación de realizar evaluaciones de impacto y de proteger la vida privada, por defecto, desde el diseño mediante funcionalidades respetuosas con los datos personales, como la posibilidad de incorporar sensores de encendido y apagado durante el vuelo y ocultación automática de áreas privadas o desdibujado de rostros cuando las imágenes han sido grabadas fortuitamente (Parlamento Europeo, Resolución sobre el uso seguro de los sistemas de aeronaves pilotadas de forma remota (RPAS) en el ámbito de la aviación civil, cit., apartados 24 y 25).

ANDERSON, D.E., "Drones and the Ethics of War", *Religion & Ethics NewsWeekly*, 14 May 2010.

BARRIENTOS, A, et al., Vehículos aéreos no tripulados para uso civil. Tecnología y aplicaciones. Universidad Politécnica de Madrid. 2007.

BENJAMIN, M., *Drone Warfare. Killing by Remote Control*, Brooklyn, Verso, , fully revised and updated, 2013.

CLARKE, R.; ROUFFAER, C. and SÉNÉCHAUD, F., "Beyond the Call of Duty: why shouldn't video game players face the same dilemmas as real soldiers?", *International Review of the Red Cross*, Vol. 94, núm. 886, 2012.

CLARKE, R., «The regulation of civilian drones' impacts on behavioural privacy», *Computer Law and Security Review*, núm. 30, 2014.

Columbia law school human rights clinic and center for civilians in conflict, *The Civilian Impact of Drones: Unexamined Costs, Unanswered Questions*, New York, 2012.

ELODI VILLENA, M., «El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración», en *Congreso Derecho TICS - SICARM 2014*, Barcelona, 23-24 de octubre de 2014.

FINN, R.L., WRIGHT, D., Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. ELSEVIER. 2012.

GUERRERO LEBRÓN, M. J., «La regulación transitoria de los operadores de aeronaves civiles pilotadas por control remoto», *La Ley mercantil*, Editorial La Ley. 31 de julio de 2014.

GUERRERO LEBRÓN , M. J., CUERNO REJADO, C., MÁRQUEZ LOBILLO, P., "Aeronaves no tripuladas: Estado de la legislación para realizar su integración en el espacio aéreo no segregado", *Revista de Derecho del Transporte,* Nº. 12, 2013.

HALLA, A.R., COYNEA, C.J., The political economy of drones. Routledge - Taylor & Francis Group. 2013.

HEYNS, C., *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Doc. ONU A/68/382, 13 de septiembre de 2013.

The Military Balance. London, The International Institute for Strategic Studies, 2014.

LEWIS, M.W., "Drones and the Boundaries of the Battlefield", *Texas International Law Journal*, Vol. 47, Issue 2, 2012.

McCLOSKEY, M., "The War Room: Daily Transition between Battle, Home Takes aToll on Drone Operators", *Stars and Stripes*, 27 October 2009,

MELZER, N., *Implications of the Usage of Drones and Unmanned Robots in Warfare*, Directorate-General for External Policies of the Union, European Union, Brussels, May 2013.

PAUNER CHULVI, C "El uso emergente de drones civiles en España. Estatuto jurídico e impacto en el derecho a la protección de datos" *Revista de Derecho Político* UNED, N.º 95, enero-abril 2016.

PEW RESEARCH CENTER, *Report questions drone use, widely unpopular globally, but not in the U.S.*, Washington, D.C., October 23, 2013.

Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston, Addendum, Study on Targeted Killings, U.N. Doc. A/HRC/14/24/Add.6.

RODRIGUEZ CANOSA, G, R., BARRIENTOS CRUZ, A; CERRO GINER, J., Caracterización de las infraestructuras críticas de exteriores y su influencia sobre sistemas de vigilancia robóticos. 2011.

SERRA CRISTÓBAL, R., «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», *Revista de Derecho Político*, núm. 92, 2015.

STERIO, M., "The United States' Use of Drones in the War on Terror: The (Il)legality of Targeted Killings Under International Law", *Case Western Reserve Journal of International Law*, Vol. 45, 2012.

SULLIVAN, J.M., Evolution or revolution? rise of uavs. IEEE Technology and Society Magazine 25(3) 2006.

UNITED STATES DEPARTMENT OF DEFENCE: U.S. *unmanned systems integrated roadmap (fiscal years 2009-2034)*, Washington DC, 2009.

VOLOVELSKY, U., «Civilian uses of unmanned aerial vehicles and the threat to the right to privacy. An Israeli case study», *Computer Law & Security Review*, núm. 30, 2014.

WATTS, A.C., AMBROSIA, V.G., HINKLEY, E.A., Unmanned aircraft systems in remote sensing and scienti_c research: Classi_cation and considerations of use. Remote Sensing. 2012.

.

CAPITULO 3

CAPITULO 3- INTELIGENCIA ESTRATÉGICA BASADA EN DATOS DE FUENTES ABIERTAS COMO RECURSO ANTE EL TERRORISMO INTERNACIONAL

1.- INTRODUCCIÓN

La información en materia de inteligencia, desde el final de la guerra fría ha sido profusamente objeto de estudio y fundamentación, y que en opinión de Matey y Navarro[167], los servicios de inteligencia[168] de cada lado del telón de acero debían prestar gran atención al desarrollo de capacidades militares del enemigo, dadas las amenazas y riesgos que caracterizan el entorno globalizado, pero actualmente resulta más complejo, dado que el final de la guerra fría supuso un incremento de los conflictos violentos a escala mundial, en donde los arraigados criterios ideológicos que alimentaban esa amenaza convencional de un bloque enemigo orgánicamente identificado y con un orden de batalla determinado, se ha trasladado hacia amenazas que desarrollan una estructura no convencional, ramificada, inestable y flexible, pero dotada de una gran voluntad de actuación, que hacen de esta volatilidad estructural su principal medio de ocultación, y que podríamos encuadrar dentro del grupo de "amenazas asimétricas"[169], que en numerosas comisiones y congresos sobre la materia han iniciado la reflexión sobre cómo adaptar la Inteligencia a los nuevos

[167] BLANCO NAVARRO, J, Mª Y DÍAZ MATEY, G.: Presente y futuro de los estudios de inteligencia en España. Documento marco IEEE .2015.

[168] Desde esta perspectiva, podemos definir por tanto la inteligencia, en la obtención de información procesada, analizada, valorada, contrastada e interpretada, destinada a fundamentar la toma de decisiones para hacer frente a riesgos u amenazas presentes o futuras que afecten tanto a los estados como a sus ciudadanos.

[169] Podemos encuadrar tales amenazas asimétricas las que se basan en la proliferación de actores no estatales en la esfera internacional y el consecuente aumento de distintos intereses contrapuestos como la lucha por los recursos escasos en donde los conflictos por los recursos naturales como el agua, petróleo, minerales estratégicos, escasez de alimento, las fuentes de energía, los conflictos separatistas o nacionalistas, las intenciones de grupos étnicos que pretenden tener su propio Estado, los conflictos entre naciones que tratan de extender sus fronteras para abarcar territorios donde habitan comunidades afines, luchas religiosas o fundamentalistas que tratan de ganar influencia y poder dentro de un mismo Estado o incluso en toda una zona geográfica, ampliando a zonas externas su poder de disuasión mediante la estrategia del terrorismo, o las guerras revolucionarias que tratan de imponer su ideología política en su propio país o en otros países de la misma región; luchas a favor de la democracia, el anticolonialismo, y las reivindicaciones indígenas; y un largo etcétera.

escenarios[170], que algunos autores han denominado guerras de cuarta generación[171].

La Guerra Asimétrica, como todo tipo de guerra o conflicto, precisa de una Inteligencia apropiada y de órganos encargados de producirla. Es aquí donde entra el ciclo de inteligencia convencional adaptándose a las necesidades del propio conflicto arrojando información que se transforma en datos concretos a disposición usualmente del mando, o de decisores políticos u organizaciones diversas, y en donde la información residenciada en internet supone una sobreabundancia de datos susceptibles de incorporarse al ciclo tradicional de inteligencia para la toma de decisiones pero que según algunos autores, esta masiva sobreinformación ha provocado que el aludido concepto tradicional de ciclo de inteligencia, este siendo cuestionado al trasladarse los esfuerzos de las agencias ya no en la obtención y procesamiento sino más bien a su análisis[172], permaneciendo abierto el debate sobre la fiabilidad, consistencia e integración que puedan configurar una visión holística e integral del trabajo de las agencias de inteligencia[173],y si cabe según matiza el citado autor, aunar esfuerzos desde los diferentes departamentos y facultades universitarias para dotar al trabajo con fuentes abiertas de información para la elaboración de inteligencia de relevancia científica y materia académica, implantando progresivamente una especialidad de inteligencia en redes abiertas al menos, en la propia formación militar profesional[174].

---

[170] DÍAZ, A.: «*La adaptación de los servicios de inteligencia al terrorismo internacional* « *ARI Nº 52-2006*

[171] LIND, W,S.: Internet World Stats: Usage and Population Statistics. Antiwar.com. (2004). En: http://goo.gl/2e3sc

[172] NAVARRO BONILLA, D.: "El ciclo de inteligencia y sus límites", *Cuadernos constitucionales de la cátedra Fadrique Furió Ceriol*, 48. 2004, pp. 51-65.

[173] UMPHRESS,D,A.: *"Naufragando en el contenedor digital: el impacto que tiene la Internet en la recopilación de inteligencia de fuentes abiertas (OSINT)"*, Air and Space Power Journal en español, 4. 2006, pp. 6-16.

[174] GARRIDO ROBRES, J,A.: *¿Sería conveniente una especialidad fundamental de inteligencia para las Fuerzas Armadas Españolas? Estudio de esta especialidad en otras Fuerzas Armadas.* Madrid, ESFAS, 2006.

2.- BIG DATA COMO HERRAMIENTA DE LA SEGURIDAD Y LA DEFENSA

De manera genérica podemos decir que la aplicación de "Big Data" a defensa y seguridad persigue capturar y utilizar grandes cantidades de datos para poder aunar sensores, percepción y decisión en sistemas autónomos, y para incrementar significativamente el que el entendimiento de la situación y contexto del analista y el combatiente o el agente del orden[175]. Para poder trabajar con la creciente complejidad y abundancia de datos, es necesario un mayor enfoque en la comprensión de la situación, especialmente en aquellos ámbitos donde los objetivos (blancos, enemigos, criminales, etc.) son en apariencia de pequeña escala y/o de carácter ambiguo. En este sentido, para un mayor cribado direccionado a la creación de inteligencia de las fuentes abiertas que trataremos, aludiremos la inteligencia denominada OSINT, acrónimo derivado de su nombre en inglés *Open-source Intelligence*[176].

Aunque *osint* ya hemos abundado no es un término nuevo, si cabe, igualmente ve necesaria su redefinición dado que la consideración que se le prestaba radicaba principalmente en que desde antaño, mantenía un concepto tradicional de recopilación de información, igualmente de fuentes abiertas, pero basado fundamentalmente en el estudio de televisión y prensa extranjera, entrevistas con los hombres de negocio o turistas a la vuelta de un viaje o colaboraciones con expertos académicos, pero que actualmente, dado el aumento de la capacidad de almacenamiento de

[175] CARRILLO RUIZ, J,A et al.: "Big data en los entornos de defensa y seguridad" documento resultado del grupo de trabajo sobre big data, de la comisión de investigación de nuevas tecnologías del centro superior de estudios de la defensa nacional. (CESEDEN) Documento de Investigación del Instituto Español de Estudios Estratégicos (IEEE) 03/2013. Pag 44.

[176] Tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público, comprendiendo cualquier tipo de contenido, fijado en cualquier clase de soporte, papel, fotográfico, magnético, óptico etc. que se transmita por el medio y que se puede acceder en modo digital o no, y a disposición pública, difundido por canales restringidos o gratuitos. Podemos considerar fuentes abiertas de ámbito OSINT:

- Datos extraíbles de la Internet abierta, frecuentemente de la web abierta.
- Estudios e informes, *white papers*, revistas especializadas y otras fuentes de literatura gris.
- Repositorios abiertos, tanto públicos como privados.
- Registros administrativos públicamente accesibles.

información residenciado en las fuentes abiertas web, y que exponencialmente ha crecido en los últimos años, genera cada día una enorme cantidad de información consciente o inconscientemente[177], evidenciándose las potencialidades de Internet y sus alcances globales, convirtiéndolo en una suerte de actor en el escenario internacional en el marco de la era de la información.

El principal documento[178] de la OTAN sobre OSINT[179] identificaba cuatro categorías en las fuentes abiertas[180]:

- OSD (Open Source Data; Datos de fuentes abiertas): impresión en bruto, radiodifusión, informe oral u otra forma de información de una fuente primaria, como una fotografía, una grabación, una imagen de satélite comercial, etc.
- OSIF (Open Source Information; Información de fuentes abiertas): integrada por datos que se agrupan generalmente por medio de un proceso de edición que proporciona algún tipo de filtrado y validación, así como una gestión de su presentación.
- OSINT (Open Source Intelligence; Inteligencia de fuentes abiertas): información que deliberadamente ha sido obtenida, discriminada, extraída y desimanada a personas seleccionadas, todo ello con objeto de responder a una pregunta o tema específico.
- OSINT Validada (OSINT-V): información a la que se puede atribuir un muy alto grado de certidumbre. Puede ser producida por un profesional de inteligencia de todo tipo de fuente, con

[177] Como por ejemplo cuando se reserva un billete de avión, se paga con una tarjeta de crédito, se entra en un servidor para ingresar el e-mail, se participa o es participado en una red social, blogs, foros de Internet o sencillamente se interactúa ante la infinidad de sensores de las ciudades inteligentes (Smart Cities).

[178] En ; http://www.nato.int/cps/en/natohq/topics_68372.htm?selectedLocale=en
OTAN Open Source Inteligencia Manual,
OTAN Open Source Inteligencia Reader
OTAN Inteligencia explotación de la Guía de Internet.

[179] El concepto OSINT, tiene su origen en los Estados Unidos como método de inteligencia analítica estandarizado y diseñado para cumplir tareas específicas o toma de decisiones de apoyo. No debe ser confundido con el OSIF, que representa toda la información a disposición del público de código abierto que se basa los análisis OSINT

[180] DAVARA RODRÍQUEZ,F.: revista *Atenea*, 12: pp. 69-71

> acceso a las clasificadas, trabajando para una nación o como personal de una coalición.

En este sentido, la creciente importancia de las fuentes abiertas ha llevado a la creación de organismos específicos como el estadounidense Open Sources Center, (OSC)[181], mientras que, en la unión europea, se han llevado a cabo iniciativas como el Eurosint[182], orientado a la cooperación europea en materia de inteligencia y al uso intensivo de las fuentes abiertas para elaborar inteligencia en la prevención de amenazas para la paz y la seguridad. O Por ejemplo uno de los think tanks más importantes del mundo; SIPRI[183] (Stockholm International Peace Research Institute) que es un instituto de estudios estratégicos, dedicado a la investigación de los conflictos, a la producción, comercio y control del armamento, al gasto militar, la prevención los conflictos, y la seguridad internacional. En el caso británico, podemos dar relevancia al NEC[184], que es una red que engloba 10 redes especializadas. Sin olvidar igualmente el potencial de la NSA[185] para abarcar también este campo de estrategia. La OTAN dispone del sistema se NNEC[186], similar en la teoría al sistema británico.

---

[181] Véase; https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

[182] Véase; https://www.eurosint.eu/

[183] Ver en: http://www.sipri.org/

[184] En el NEC británico hay un enlace directo entre el nivel Estratégico y el Táctico, lo que abunda en la idea de que en las situaciones actuales de "asimetría", el nivel Táctico se convierte, muchas veces, en Operativo y que los medios tecnológicos del nivel Estratégico pueden trabajar directamente para el Táctico.

[185] La (NSA) National Security Agency es responsable de la protección, desarrollo y control de las comunicaciones militares y administrativas, el desarrollo de las tecnologías de la información, la seguridad de las redes informáticas, el espionaje vía satélite y la coordinación de la guerra en el espacio, entre los Estados Unidos y los servicios de información de Reino Unido, Canadá, Australia y Nueva Zelanda entre otros. En todo el mundo, todas las comunicaciones por correo electrónico, teléfono y fax son regularmente interceptadas por Echelon, cuyos ordenadores extraen de la masa de informaciones los mensajes que contengan palabras-clave sensibles".

[186] Para la OTAN, el NNEC representa el enfoque y la política común para armonizar el uso de las nuevas tecnologías, con la finalidad de usarlas en futuras misiones. El problema que se planteará es que la OTAN no tiene órganos propios de Inteligencia y que depende de los de las naciones aliadas.

3.- LA ADQUISICIÓN DE INTELIGENCIA A PARTIR DE LAS NUEVAS TECNOLOGÍAS QUE ALMACENAN DATOS Y SU ENCUADRE DENTRO DE LA ESTRATEGIA

Actualmente, los sistemas de ayuda al mando en la toma de decisiones, formados fundamental por los órganos de inteligencia, están evolucionando hacia un "sistema de sistemas", en el que se integran en una única red sensores, decisores, plataformas varias e inteligencia, con la finalidad de aumentar la capacidad de acción de las fuerzas por una mejor explotación de la información, mediante la superioridad que supone la obtención de información relevante y decisiva para el combate, a través de la explotación oportuna de inteligencia, siendo válido tanto para la batalla convencional como para el enfrentamiento asimétrico.

En la inteligencia de código abierto, la recopilación de información difiere generalmente de las diferentes disciplinas de la inteligencia que hemos referenciado, consolidándose en las agencias de inteligencia una nueva conceptualización de la estrategia operacional basada en estos recursos, básicamente porque la obtención de información en bruto a analizar puede ser un desafío importante, especialmente si son objetivos no cooperativos, independientemente este residenciada en fuentes abiertas[187] o en la minería de datos[188]. En este mismo contexto de fuentes abiertas, se está

[187] Por su parte MARTÍN DE SANTOS, I. Y VEGA, A. M.: «Las fuentes abiertas de información: un sistema de competencia perfecta», en Inteligencia y Seguridad: revista de análisis y prospectiva, número 8, pp. 91-112, junio-noviembre de 2010. "Las fuentes abiertas de información incluyen tanto la Internet superficial como la profunda (también llamada invisible), el correo electrónico, así como las fuentes de los medios de comunicación tradicionales, incluyendo los medios dirigidos a un público específico y boletines especializados y de los foros de discusión en línea. Se incluye la literatura gris, expertos (o especialistas) en determinados temas y cualquier persona que tenga conocimiento de algo por haber sido testigo directo de ello o haberlo vivido". Por otra parte, IRAVEDRA, J. C.: «Inteligencia de fuentes abiertas en la Unión Europea (proyecto Virtuoso)», Jornadas de Estudios de Seguridad, 17, 18 y 19 mayo de 2011, La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a amenazas, Instituto Universitario «General Gutiérrez Mellado»- Universidad Nacional de Educación a Distancia, Madrid, 2011. dice que: "Fuentes abiertas son las que no están clasificadas".

[188] La minería de datos o data mining o "el arte de sacar conocimiento de grandes volúmenes de datos" es una técnica que "consiste en extraer información de los algoritmos que contienen las grandes bases de datos que acumulan la historia de las actividades de las organizaciones" MARTÍNEZ, GILBERTO L.: "Minería de datos: Cómo hallar una aguja en un pajar", Ingenierías, 53 2011. págs. 55-63 Las redes de transmisiones digitalizadas, con su gran capacidad y velocidad

produciendo un gran movimiento alrededor de lo que se conoce como Open Data, implicando que los datos puedan ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen, siendo sus características fundamentales las siguientes:

- Disponibilidad y acceso: la información debe estar disponible como un todo y a un costo razonable de reproducción, preferiblemente descargándola de internet. Además, la información debe estar disponible en una forma conveniente y modificable.
- Reutilización y redistribución: los datos deben ser provistos bajo términos que permitan reutilizarlos y redistribuirlos, e incluso integrarlos con otros conjuntos de datos.
- Participación universal: todos deben poder utilizar, reutilizar y redistribuir la información.

El termino recientemente acuñado en el diccionario LID de Inteligencia y Seguridad[189] de (SOCMINT) y definido como la "actividad de inteligencia referida a las redes sociales y medios sociales de comunicación de plataforma digital y los datos que las mismas generan" y que podríamos esquematizarlo según Álvarez y Perdomo[190] como la interacción entre las funciones y roles de las redes sociales, vuelcan la Inteligencia de Fuentes Abiertas (OSINT), creándose la Inteligencia en Redes Sociales (SOCMINT), las interrelaciones entre los medios de comunicación tradicionales y los medios con soportes en redes sociales y web 2.0 (social media + mass media), las operaciones de activismo en la red (hactivism) y la ingeniería social.

---

de transmisión, permiten que las comunicaciones tácticas y, dentro de ellas, de las utilizadas por los órganos de Inteligencia. Como ejemplo; en la primera guerra de Irak, una fuerza de 500.000 hombres disponía de 100Mbits de banda ancha; unos 12 años más tarde, los 350.000 combatientes de la "Operation Irak Freedom", en la segunda guerra de Irak se apoyaban en 3.000Mbits.

[189]Vease:https://www.google.es/search?q=dicionario+LID+inteligencia&ie=utf-8&oe=utf-8&gws_rd=cr&ei=iX3UVbu8CobnUtTUr8gN#q=diccionario+lid+inteligencia+y+seguridad+pdf

[190] ALVAREZ ALVAREZ, L, A Y PERDOMO CORDERO, C.: "Inteligencia, Cibereguridad y Ciberdefensa; nuevas implicaciones conceptuales en las Estrategias de Seguridad Nacional." Universidad de Las Palmas de Gran Canaria, ULPGC.2002.

La web 2.0 supuso un cambio en el modo de comunicación de los usuarios en Internet, de forma que los usuarios dejan de ser meros receptores de información y comienzan a ser generadores de la misma, como ejemplo lo supone el que hoy en día, la mayor parte de los usuarios forman parte de las redes sociales, disponen de sus propios blogs o participan en foros que provoca que el volumen de información disponible haya crecido de forma exponencial en los últimos años.

Este bruto ingente de información[191] que se puede obtener a través de la obtención, gestión, integración, análisis, filtrado, refinamiento y síntesis de la información ubicada en todo tipo de soportes y formas de transmisión y comunicación de información en las fuentes web[192], se cimenta generalmente en el pasado, pero a los efectos de obtener inteligencia es útil para comprender el presente y hacer predicciones futuras, ya que normalmente las decisiones se basan en experiencias pasadas, siendo posible identificar tendencias, anomalías y amenazas, destacándose por tanto la importancia del papel de los profesionales que gestionen estas fuentes, aplicadas a la seguridad, la defensa nacional así como la toma de decisiones en general.

Por su parte, OSINT acrónimo derivado de su nombre en inglés *Open-*

[191] La proliferación del uso de Internet y la facilidad de publicación de contenidos a través de diferentes medios como redes sociales o blogs ha favorecido que se almacene una ingente cantidad de información online. Las cifras más significativas son las siguientes:

- Usuarios de Internet; aproximadamente 2.500 millones de usuarios.
- Únicamente el servidor Google, almacena 30 billones de páginas web, o lo que es lo mismo, más de 1.000 terabytes de información
- La red social Facebook tiene más de 1.000 millones de usuarios, 60 millones de páginas y 270.000 millones de fotos subidas.
- La red social Twitter tiene cerca de 240 millones de usuarios activos que escriben diariamente cerca de 600 millones de tweets.
- La red social Tumblr tiene cerca de 180 millones de blogs y alrededor de 55.000 millones de posts.
- La red social Flickr tiene casi 90 millones de usuarios y más de 10.000 millones de fotos.
- La red social Instagram cuenta con más de 350 millones de usuarios activos, que han subido 30 billones de fotos desde el 2010. Aproximadamente se suben a la red social 5 millones de fotos diariamente

Estos son algunos de los datos representativos más conocidos, sin mencionar la cantidad de información disponible en la DEEP WEB, así como también aquella información no accesible para el usuario común, pero existente dentro de la Web en capas invisibles o profundas, cuyos contenidos no son accesibles desde motores de búsqueda comunes y conocida como *WEB DATA MINING*.

[192] No olvidemos que la World Wide Web tiene un origen como experimento y herramienta militar.

source Intelligence[193] en los últimos años, a causa del desarrollo tecnológico en la era de la información, la inteligencia *osint* amplía su rango de acción a una clase de Inteligencia que tiene por objeto la realización de productos de valor añadido a partir de información procedente igualmente de fuentes abiertas como las descritas, y particularmente las fuentes abiertas residenciadas en páginas web, contribuyendo así a ampliar el rango de necesidades actuales de información, como producto de inteligencia, que en su defecto, o sin dedicarle la atención oportuna, esta corre el riesgo de estar permanentemente desactualizada.

Determinados los alcances e importancia de OSINT, hemos de revelar nuevamente que este no es un concepto moderno, siquiera en su actual entendimiento, pues ya desde hace más de una década, la OTAN, le concede especial relevancia, como lo evidencia el ejemplo del programa (EUSC) formado por un centro de satélites dedicado a la producción y explotación de inteligencia a partir de información de origen espacial, por medio del análisis de datos de satélites comerciales. También la Agencia Europea de Defensa (EDA) ha puesto en marcha programas de desarrollo de herramientas de prospectiva y análisis OSINF y de formación de inteligencia OSINT.

En este sentido y como impulsor, destaca principalmente los Estados Unidos, cuyos servicios de inteligencia han concedido una gran importancia a OSINT, mediante la transformación, en 2005, del Servicio de Información de Emisiones del Exterior (FBIS) en el Centro de Fuentes Abiertas (OSC), incorporado OSIF y OSINT, en sus rutinas de Inteligencia militar implantado la red IKN (Intelligence Knowledge Network) proporcionando servicios de inteligencia al Ejército. Francia, por su parte está impulsando la plataforma HERISSON (Habile Extraction du

[193] Tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público, comprendiendo cualquier tipo de contenido, fijado en cualquier clase de soporte, papel, fotográfico, magnético, óptico etc. que se transmita por el medio y que se puede acceder en modo digital o no, y a disposición pública, difundido por canales restringidos o gratuitos. Podemos considerar fuentes abiertas de ámbito OSINT:

- Datos extraíbles de la Internet abierta, frecuentemente de la web abierta.
- Estudios e informes, *white papers*, revistas especializadas y otras fuentes de literatura gris.
- Repositorios abiertos, tanto públicos como privados.
- Registros administrativos públicamente accesibles.

Renseignement d´intéret Stratégique a partir de Sources Ouvertes Numérisées) de integración de información de fuentes abiertas. Veremos en el siguiente epígrafe algunas otras más relevantes al respecto de inteligencia militar.

- Requisitos: En esta etapa se establecen los parametros minimos y maximos que deben satisfacerse para conseguir el objetivo que ha activado el desarrollo del sistema.
- Fuentes de información: Esta etapa consiste en identificar a partir de los parametros establecidos, las fuentes de interés que serán recopiladas.
- Adquisición: En esta etapa se obtiene la información a partir de los orígenes indicados.
- Procesamiento: Esta etapa consiste en dar formato a toda la información recopilada para que posteriormente pueda ser analizada discriminandola del bruto obtenido.
- Análisis: En esta etapa se genera inteligencia a partir de los datos recopilados y procesados, habiendo relacionado la información buscando los patrones que permitan llegar a conclusiones significativas.
- Inteligencia: Esta etapa consiste en presentar la información potencialmente útil y comprensible, para que pueda ser correctamente explotada

4.- RELEVANCIA ESTRATÉGICA DE LAS BASES DE DATOS EN FUENTES ABIERTAS

La doctrina discute acaloradamente tanto los beneficios de la web como los perjuicios que esta supone pues el acceso de la información no es ajeno a ser utilizada de modo legal o ilegal no pudiendo discriminar ningún servidos hasta la fecha la calidad del demandante de información. Este será un reto de futuro para la WWW, poder discriminar el usuario final, basándose igualmente en las propias informaciones web para detectar quien es el usuario final o al menos si se discute la utilización más o menos

legal de la información a la que accede. Estas son bases de datos que indizan estáticamente sus páginas por lo que cuando buscamos información en cualquiera de los buscadores propuestos, únicamente se arroja información que pueda esta residenciada en ese buscador, omitiéndose gran cantidad de información residenciada en las restantes webs, así como en el internet profundo propio de la estructura de la *World Wide Web* en forma de tela de araña que aunque pueda enlazar unas páginas con otras, hace que aquellas que no tengan enlaces indexados propios, no puedan ser localizados por los motores de búsqueda aunque si permanezcan en la parte invisible de la Red.

También podemos utilizar los enlaces que aparecen en las páginas *web* de instituciones o *think tank*, mas importantes de referencia etc. por ejemplo *Completeplanet*[194] que tiene un apartado específico para bases de datos de temas militares, así como especialmente la página SIPRI[195], *(Stockholm International Peace Research Institute) que* es un instituto internacional de estudios estratégicos, dedicado a la investigación de los conflictos y al control de armamento y al desarme.

En la página *web* de SIPRI podemos consultar seis bases de datos.

SIPRI Facts on International Relations and Security Trends

Base de datos que ofrece información sobre las relaciones internacionales y las tendencias de seguridad.

SIPRI Multilateral Peace Operations Database

Base de datos que ofrece información sobre todas las operaciones de paz llevadas a cabo desde el año 2000, incluyendo la ubicación, las fechas de implementación y el funcionamiento, el mandato bajo el que se llevan a cabo, países participantes, el número de personas empleadas, costes económicos y bajas.

SIPRI Military Expenditure Database

Base de datos que ofrece que recoge información sobre el gasto militar de 172 países desde el año 1988.

SIPRI Arms Transfers Database

[194] Ver: *http://aip.completeplanet.com/*
[195] Ver: *http:// www.sipri.org/databases*

Base de datos sobre transferencias internacionales de armas, agrupadas en siete categorías de armas convencionales.

SIPRI Arms Embargoes Database

Base de datos que ofrece información sobre todos los embargos de armas que han sido llevados a cabo por una organización internacional, como la Unión Europea o la Organización de Naciones Unidas, desde 1998.

SIPRI National Reports Database

Base de datos que proporciona enlaces a todos los informes nacionales de acceso público sobre exportaciones de armas.

Otra página relevante en cuanto a información de interés para el analista de inteligencia lo supone *Jane's Intelligence Centre*. Que dispone de una ingente cobertura informativa sobre todos los aspectos relacionados con la defensa, la seguridad y las Fuerzas Armadas a nivel mundial, etc, Resultando de gran utilidad para encontrar información por ejemplo: presupuestos de los principales países del mundo en cuestiones de defensa, perfiles de países con una completa información sobre su situación política, económica, demográfica, militar, etc. imágenes sobre buques, vehículos terrestres y aviones, y sus detalles así como cuales vehículos militares, aeronaves y buques van a adquirir en el futuro a corto y medio plazo los principales países del mundo o información sobre las amenazas y riesgos que experimentan los principales países del mundo y qué capacidad tienen dichos países para hacer frente a estas amenazas: estabilidad de los Estados, crimen organizado, terrorismo, insurgencia, relaciones internacionales, etc. datos de contacto e información sobre organizaciones de la industria aeroespacial y de la industria de la defensa: instituciones gubernamentales, fabricantes, distribuidores, compañías de servicios, etc.

Otra página relevante en cuanto a información lo supone el *GDI (Global Defense Information)* que es una base de datos sobre defensa y tecnología aeroespacial que contiene artículos y noticias sobre el sector.

También la página *ISCTRC (International Security And Counter Terrorism Reference Center)* proporciona información sobre todos los aspectos relacionados con la seguridad y la lucha contra el terrorismo. En la misma línea la página *ProQuest Military Collection* es igualmente una base

de datos especializada en seguridad y defensa, aeronáutica y vuelos espaciales, comunicaciones e ingeniería civil.

La página *Armed Conflict Database está elaborada por el International Institute for Strategic Studies de Londres* es una base de datos que proporciona información sobre países en los que existe o ha existido algún conflicto bélico o actividad de grupos terroristas desde el año 1997. La página *Europa World Plus* cubre información política y económica de más de 250 países y territorios, desde Afganistán hasta Zimbabue. The Europa Regional Surveys of the World, aportando datos sobre los gobiernos, enlaces a otras instituciones, artículos, etc. La página *INS (International Relations and Security Network)* es un proyecto del CSS *(Center for Security Studies),* en el ETH *(Swiss Federal Institute of Technology)* de Zurich, financiado conjuntamente por el Departamento Suizo de Defensa, Protección Civil y Deporte (DDPS) y ETH Zurich (Escuela Politécnica Federal). Y en donde podemos encontrar, *think tanks*, agencias gubernamentales, organizaciones internacionales, organizaciones no gubernamentales información sobre el cambio climático, los movimientos migratorios, la seguridad alimenticia, e instituciones privadas.

Otra página interesante lo representa la *World Security Network,* que es una organización internacional, independiente, sin fines de lucro que tratan las relaciones internacionales, temas puramente militares en cuanto al estudio de los conflictos, las operaciones de paz, los costes de las mismas y las políticas de seguridad.Forman parte de esta red instituciones como OTAN, el Center for Strategic and International Studies, la Defence Academy of the United Kingdom, el International Institute for Strategic Studies, la National Defense University, y UNISCI.

Como observamos al alcance de un clik tenemos fuentes de información abiertas, que pueden proveer de casi un 90% de la información necesaria para la toma de decisiones (deliberadamente buenas o deliberadamente malas) y para el diseño de políticas. Queda abierto por tanto el debate en dos sentidos, por un lado establecer si la sobreexposición de información relevante por parte de los gobiernos y entes sobre sus políticas de defensa y sus industrias armamentísticas así como su declarado potencial de defensa, resulta antagónico con el propio carácter que se le

debe suponer a tales asuntos, dado el desconocido perfil que pueda acceder a la información para ser usada con fines de dudosa confiabilidad, y por otro lado deberá acontecer desde el ámbito militar y el ámbito académico-legal un interesante debate para adelantar los parámetros que dilucidaran las respuesta de la inteligencia sobre los fenómenos y retos de la inteligencia que se avecinan, tales como las plataformas informáticas cuánticas, la guerra informática y digital o la ingeniería armamentista basada en la computación, las potencialidades de Internet y las fuentes abiertas de información en línea.

5.- REFERENCIAS

ALVAREZ ALVAREZ, L,A Y PERDOMO CORDERO,C.: "Inteligencia, Cibereguridad y Ciberdefensa; nuevas implicaciones conceptuales en las Estrategias de Seguridad Nacional." 2015

BLANCO NAVARRO, J, Mª Y DÍAZ MATEY, G.: Presente y futuro de los estudios de inteligencia en España. Documento marco IEEE .2015

CARRILLO RUIZ, J,A et al.: "Big data en los entornos de defensa y seguridad" documento resultado del grupo de trabajo sobre big data, de la comisión de investigación de nuevas tecnologías del centro superior de estudios de la defensa nacional. (CESEDEN) Documento de Investigación del Instituto Español de Estudios Estratégicos (IEEE) 03/2013.

DÍAZ, A.: «*La adaptación de los servicios de inteligencia al terrorismo internacional* « *ARI Nº 52-2006* -

GARRIDO ROBRES, J,A.: *¿Sería conveniente una especialidad fundamental de inteligencia para las Fuerzas Armadas Españolas? Estudio de esta especialidad en otras Fuerzas Armadas*. Madrid, ESFAS, 2006.

IRAVEDRA, J. C.: «Inteligencia de fuentes abiertas en la Unión Europea (proyecto Virtuoso)», Jornadas de Estudios de Seguridad, 17, 18 y 19 mayo de 2011

LIND, W,S.: Internet World Stats: Usage and Population Statistics. Antiwar. 2004.

MARTÍN DE SANTOS, I. Y VEGA, A. M.: «Las fuentes abiertas de

información: un sistema de competencia perfecta», en Inteligencia y Seguridad: revista de análisis y prospectiva, número 8, pp. 91-112, junio-noviembre de 2010

MARTÍNEZ, GILBERTO L.: "Minería de datos: Cómo hallar una aguja en un pajar", Ingenierías, 53 2011. págs. 55-63

NAVARRO, D. El ciclo de inteligencia y sus límites. *Cuadernos Constitucionales de la Catedra Fadrique Furió Ceriol, Vol. 48*. 2004.

UMPHRESS,D,A.: "Naufragando en el contenedor digital: el impacto que tiene la Internet en la recopilación de inteligencia de fuentes abiertas (OSINT)", Air and Space Power Journal en español, 4. 2006, pp. 6-16

CAPITULO 4

CAPITULO 4 - IDONEIDAD DE LA VIDEO-VIGILANCIA EN EVENTOS PÚBLICOS Y PRIVADOS Y SU IMPACTO EN LA LEGISLACIÓN DE PROTECCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

La seguridad de las personas es un tema de creciente preocupación por parte de los Gobiernos y las autoridades, promoviéndose a raíz de fatídicos acontecimientos acaecidos en atentados terroristas o calamidades sucedidas en diversos eventos[1], han convirtiendo en una prioridad a nivel mundial, la necesidad de potenciar la seguridad de la comunidad y de los individuos. Con objeto de lograr y ofrecer una mayor percepción de seguridad, hemos dotado nuestras ciudades de dispositivos capaces de monitorizar todas nuestras actuaciones, desde la esfera pública ya sea con fines de seguridad, persecución de los delitos o el control del tráfico, o desde el ámbito privado, mediante la vigilancia y control de zonas privadas, zonas residenciales o eventos desarrollados en locales o recintos abiertos al público. Esta suerte de videocontrol, genera, inquietudes y reflexiones que pueden colisionar con algunas garantías del estado de derecho. A su vez igualmente de lograr un mayor sentimiento de seguridad se ha impulsado por parte de los gobiernos al diseño de sistemas de seguridad y video-vigilancia mediante inteligencia artificial basada en sensores y algoritmos inteligentes con capacidad de determinar mediante la visión por computación, tanto nuestros movimientos y preferencias, o nuestro reconocimiento biométrico, como incluso realizar seguimientos aleatorios y automáticos de objetos y sujetos, con objeto de ofrecer "soluciones inteligentes", capaces de interpretar incluso, la posible comisión de un delito o de un acto que pudiere generar inseguridad pública, convirtiendo nuestras calles en una especie de panóptico[2] digital donde los ciudadanos están monitorizados a tiempo real, y en donde el mundo de la tecnología no ha sido ajeno a esta implementación de avances incorporando similares prestaciones, en cualquier dispositivo inteligente, dotado de una cámara. Todas estas infraestructuras digitales generan reflexiones e inquietudes que pueden colisionar con algunas garantías del estado de derecho. Los

objetivos principales empleados para la confección y análisis de este artículo se apoyaran en las siguientes cuestiones;

a) Elaboración de un estado del arte sobre la evolución de los sistemas de vigilancia que incluya los primeros sistemas de CCTV más rudimentarios hasta los más avanzados abundando en sus características, donde la mejora y adición de nuevas funcionalidades suponen un reto para la comunidad jurídica detallado las etapas de este tipo de sistemas.

b) La regulación jurídica que conocemos, al respecto de la videovigilancia o tratamiento de la imagen concreto, esta descrita en base a unos medios técnicos preexistentes que pueden mostrarse insuficientes para abarcar los nuevos avances de la tecnología y no son pocas las confusiones o lagunas jurídicas afectadas por la evolución tecnológica, dilucidando si los novedosos métodos de videovigilancia, se acomodan al corpus legal actual.

2. EVOLUCIÓN DE LOS SISTEMAS DE VIDEOVIGILANCIA

El uso de la video-vigilancia tuvo sus inicios en la década de los años cincuenta en diversas ciudades de Alemania con objeto de controlar el fluido del tráfico, trasladándose sus usos en décadas posteriores al control de manifestaciones y desordenes públicos en ciudades de Estados Unidos y del Reino Unido. En España, el uso de video-vigilancia fue introducido a partir de la década de los noventa inicialmente por las policías locales, y posteriormente por las policías autonómicas y policías estatales para el control de viales y el fluido del tráfico, evolucionando su utilización en los últimos años, al diseño de sistemas de seguridad monitorizados mediante cámaras, con la intención de otorgar un mayor grado de seguridad y control sobre los procesos de vigilancia tradicionales con el objeto de anticiparse a corroborar acontecimientos delictivos. Inicialmente este control sobre las cámaras de video-vigilancia era ofrecido y controlado por la administración, pero en los últimos años parte de ese control se trasladó a

las empresas de seguridad privada dada la híper-evolución y asunción de servicios que aglutinaban estas, siendo utilizadas desde entonces, para el control tanto público como privado de áreas indistintamente de titularidad pública o privada. Con este objetivo inicial de las autoridades para controlar aspectos preocupantes como el fluido del tráfico o algunas áreas de transito ciudadano, los primeros sistemas de vigilancia monitorizada y todavía hoy vigentes, se denominan sistemas CCTV (circuito cerrado de televisión), estando caracterizados como un sistema de tecnología de vigilancia visual que implica la instalación de una red de cámaras de grabación, fijas o móviles, en lugares estratégicos, que enviaban la señal captada a uno o varios monitores en otro punto de la instalación. Las imágenes recibidas podían ser almacenadas en un equipo videograbador para su análisis posterior, en donde un personal de seguridad público o privado, observaba lo monitorizado en tiempo real o diferido. Estos sistemas, permitían la monitorización de los puntos más vulnerables y estratégicos de un determinado entorno, siendo implantados en multitud de lugares ayudando a la detección de posibles intrusiones, acciones malintencionadas o situaciones de riesgo para la ciudadanía, pero su talón de Aquiles lo representaba la dependencia absoluta de la actividad humana en donde los factores como la fatiga acumulada tras varias horas de trabajo, la dificultad de observar varios monitores al mismo tiempo o el propio sesgo humano, reducían considerablemente la probabilidad de detectar todas las situaciones anómalas.

En los últimos años, la evolución constante de la tecnología, y el abaratamiento de esta, han impulsado el interés de investigadores por crear propuestas de nuevos sistemas de seguridad evolucionados que puedan trabajar de forma semiautomática y con capacidad para tomar decisiones por sí mismos, clasificando esta evolución según Valera y Velastin(2005), en tres generaciones de acuerdo a las tecnologías que emplean, así como las ventajas y los problemas que representan.

Los aludidos sistemas de CCTV, y que ahora vamos a denominar de primera generación, están formados por un conjunto de cámaras enlazadas unas con otras denominándolo circuito cerrado, y distribuidas a lo largo del entorno vigilado, estando a su vez conectadas a un conjunto de monitores

ubicados en una sala central donde un sujeto controla el entorno determinado. El principal sesgo que se le atribuyen a estos sistemas de primera generación es que su actividad es fundamentalmente reactiva, radicada en la dependencia absoluta de la actividad y observación humana, amparados en la consideración y criterio que en cada momento le fuera otorgado por el observador en la captación del suceso sospechoso de ser delictivo, desestimándose cualquier otra información por parte del sistema, que no tuviera visos de peligrosidad, añadiéndose a este sesgo, los estudios que demuestran que el rendimiento de una persona observando un monitor disminuye notablemente tras 20 minutos de vigilancia, el siguiente problema que presentan estos sistemas de primera generación lo representan en que utilizan técnicas analógicas para la distribución y almacenamiento de imágenes realizándolo mediante grabadores de vídeo, dificultando en gran medida el mantenimiento intensivo del sistema, así como la posibilidad de acceso remoto o la integración con otros sistemas.

A pesar de las deficiencias descritas, estos sistemas de primera generación todavía son ampliamente utilizados en todo el mundo, en donde se han incluido algunas mejoras digitales como el control remoto de zoom, visión nocturna o la detección de movimiento que permite en este último caso, pasar al sistema a un modo de alerta. Según estos motivos descritos, y basándonos en las demandas del sector de la seguridad, la vídeo vigilancia tradicional tiene ciertas dificultades para cumplir cada vez más las mayores exigencias del sector, surgiendo la necesidad de crear sistemas de seguridad más eficaces, para mejorar su efectividad y aliviar la carga y sesgo del operador humano. Determinadas las necesidades por parte de los expertos en seguridad, se han promovido acciones para intentar crear sistemas de vigilancia inteligentes, y que denominaremos de segunda generación y tercera generación.

Los sistemas de video-vigilancia de segunda generación, son una combinación de los sistemas tradicionales de CCTV, con una serie de mejoras que los convierten en computadoras basadas en inteligencia artificial. Cuando el equipo de CCTV está conectado a una red IP, es posible visualizar las imágenes, almacenadas o en tiempo real, mediante Internet. Por tanto la mejora en la segunda generación de video-vigilancia mediante

la vídeo-vigilancia IP es una tecnología que combina los beneficios analógicos de los tradicionales CCTV con las ventajas digitales de las redes de comunicación IP (Internet Protocol), permitiendo la supervisión local o remota de imágenes así como el tratamiento digital de las imágenes, para el visionado en directo y grabación ininterrumpida durante períodos programados, reduciendo la dependencia que existe con la actividad humana, interpretando en la medida de lo posible los eventos y comportamientos que se producen en el entorno monitorizado reduciendo la incertidumbre y la vaguedad del observador.

Por lo tanto, los sistemas de seguridad de segunda generación mejoran las prestaciones de los de la primera, cuando tienen la capacidad de alertar al personal de seguridad sobre lo que ocurre, al utilizar algoritmos eficientes que interpretan en un tiempo cercano al real el evento monitorizado.

Los sistemas de video-vigilancia de tercera generación utilizan los avances de las dos generaciones anteriores y están formados por un amplio repertorio de sensores distribuidos geográficamente por todo el entorno observado, transmitiendo información de forma simultánea en tiempo real ofreciendo mayores garantías de responder en tiempo real y con la capacidad de interpretar en la escena monitorizada el reconocimiento biométrico, y el movimiento considerado anómalo basado en sus comportamientos, sin necesidad de contar con la atención del operador humano.

Actualmente diversos equipos de investigación en universidades españolas[3], y europeas están impulsando mediante el desarrollo de plataformas de hardware/software plataformas de localización y procesado de vídeo inteligente, que tiene por objeto estudiar y validar las nuevas tecnologías de movilidad, localización y procesado de vídeo para poder ofrecer nuevos servicios a la ciudadanía, tales como las posibilidades ofrecidas desde líneas de investigación que podrían ser usadas tanto de forma independiente como añadida a los actuales CCTV, telefonía móvil y a los llamados wearables, dispositivos electrónicos que se 'llevan puestos', como gafas, relojes o pulseras inteligentes, vehículos autónomos, drones aéreos no tripulados, videovigilancia privada etc.

Como hemos observado, los sistemas más novedosos de video-vigilancia, si bien pueden presentar importantes mejoras respecto a los sistemas de primera generación que posibilitan una mayor eficacia en la lucha contra el crimen o la mejora de la calidad y percepción de la seguridad, su evolución técnica presenta discrepancias que superan el espectro legista, evidenciando carencias de encaje jurídico y vacío legal respecto al incremento de las nuevas posibilidades que la técnica ofrece.

Obviando por el momento este escenario que se está desarrollando sobre las nuevas posibilidades de la videovigilancia, veamos el estado actual legal sobre la videovigilancia tal y como el legislador la entiende y ejecuta.

3. VIDEO-VIGILANCIA REALIZADA POR LAS FUERZAS Y CUERPOS DE SEGURIDAD

No están totalmente resueltas jurídicamente las consideraciones que suscita la video-vigilancia en las zonas urbanas o en cualquier evento público, dado que su híper-utilización, colisiona directamente con derechos fundamentales de especial protección, tales como el derecho a la intimidad o a la propia imagen. Con intención de dotar de una base jurídica al incipiente uso de la video-vigilancia en el ámbito público, y respondiendo a la Directiva 95/46/CE, fue sancionada la Ley orgánica 4/1997 de 4 de agosto, reconociéndose en su art 2, la necesidad de establecer la legitimidad, la adecuación y la proporcionalidad en el uso de la video-vigilancia, respetando el contenido esencial de los derechos fundamentales afectados, mientras que el Real Decreto 596/1999 de 16 de abril por el que se regula la citada ley orgánica, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, dispone que las cámaras de video-vigilancia deberán utilizarse siempre con respeto al principio de proporcionalidad en su doble versión de idoneidad y de intervención mínima, correspondiendo a las Administraciones publicas autorizar la instalación y uso de tales dispositivos, desprendiéndose que en la vía pública, la titularidad para instalar, mantener y utilizar las cámaras de video-vigilancia es potestad de la seguridad pública.

Recordemos que la Ley 4/1997 alude que su finalidad es regular la utilización de la video-vigilancia por parte de las fuerzas y cuerpos de seguridad públicos, esto es, omitiendo directamente a la seguridad privada en su tratamiento, cuestión esta que no impide que pueda ser un equipo de seguridad privada el que controle la recepción de imagen o como expone Arzoz (2010), actualmente resulta difícil diferenciar entre las instalaciones de seguridad pública y privada ya no solo por la obligada subordinación de la seguridad privada con la pública, sino que generalmente, muchas instalaciones públicas, recurren a los servicios de la seguridad privada para su control y mantenimiento, como una suerte de privatización de la seguridad pública, cuestión esta que referiremos en adelante.

Reconocida la ambigüedad legista del alcance y limites en el uso de la video-vigilancia, y la falta de una base jurídica concisa en la legislación actual, entiende parte de la jurisprudencia a través de sentencias al efecto, que si bien resulta un medio invasivo, resulta legítimo monitorizar en la vía pública, escenas y acontecimientos presuntamente delictivos, desprendiéndose del enunciado del art 1.1 de la Ley, que aun considerando motivos de seguridad pública, la utilización de la video-vigilancia por las Fuerzas y Cuerpos de Seguridad, deberá respetar el principio de proporcionalidad solventando a su vez, las necesidades de idoneidad y de intervención mínima[4], que exigirá la existencia de un riesgo razonable para la utilización de video-vigilancia y que en ningún caso, podrán tomarse imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, así como tampoco se podrán grabar conversaciones de naturaleza estrictamente privada, salvo consentimiento del titular o autorización judicial, siquiera, en lugares públicos, abiertos o cerrados, cuando se afecte de forma directa y grave a la intimidad de las personas, respetándose escrupulosamente las normas relacionadas con el periodo de conservación de imágenes, destrucción de estas, o su revelación y puesta a disposición de las autoridades judiciales o administrativas.

Como se observa, la norma legal distingue las facultades otorgadas a los cuerpos y fuerzas de seguridad, para filmar la actividad humana en los lugares púbicos, en función de la labor encomendada a estos cuerpos, que como hemos indicado es: la prevención de la delincuencia, mediante el

oportuno mantenimiento de la seguridad ciudadana y el orden público, y la represión y averiguación del delito, entendiendo las labores preventivas como aquellas que se recogen tanto en la LO 4/1997 desarrolladas por su reglamento 596/1999, tratando de conseguir según define el art 1, la utilización pacífica de vías y espacios públicos y la prevención de delitos, faltas e infracciones relacionadas con la seguridad pública, mediante, entre otras, la captación, reproducción y tratamiento de imágenes y sonido, de forma que sin embargo no supongan una intromisión ilegítima del derecho a la propia imagen de los ciudadanos así afectados prevenido en el art. 2,2 LOPH 1/1982 de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En consecuencia, la norma autoriza la instalación tanto de cámaras estables como móviles en espacios públicos, bajo la existencia de un riesgo razonable para la seguridad publica en el caso de las cámaras fijas y de un peligro concreto para el uso de las cámaras móviles, todo ello conforme a las ponderaciones y exigencias racionales de proporcionalidad e idoneidad y que veremos en el apartado dedicado expresamente al valor probatorio de la prueba videográfica. La Ley 4/1997 indica que respecto al establecimiento de cámaras fijas en lugares públicos, se requerirá la previa autorización del Delegado del Gobierno en la Comunidad Autónoma, previo informe favorable de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la Comunidad Autónoma respectivamente, pero algo menos concreto resulta el trámite de autorización de cámaras móviles, que requieren únicamente la autorización del máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad del Estado, quien lo pondrá en conocimiento de la comisión en un plazo de setenta y dos horas según el art. 5.2.

Veamos a continuación la particularidad que rige respecto a la seguridad privada siendo procedente describirla seguidamente de la seguridad pública, con objeto de observar tanto las diferencias como las particularidades que hacen de la video-vigilancia un constructo en el que ambas tienen difícil separación legal, al poder colisionar ambos durante su ejecución y desarrollo, con aspectos fundamentales que dificultarían su procedencia.

4. CONSIDERACIONES SOBRE LA VIDEO-VIGILANCIA REALIZADA POR LA SEGURIDAD PRIVADA

Detallan las estadísticas que la evolución de la seguridad privada promueve la extensión de la video-vigilancia de un modo mucho más acelerado que la que pudiere suponer la video-vigilancia pública, evidenciado por la ingente cantidad de ficheros inscritos bajo este carácter. Tanto en lugares cerrados públicos, como en lugares privados, es frecuente la existencia de cámaras, instaladas con un fin de seguridad y vigilancia. Dentro de este grupo, y por lo que se refiere a la ley de protección de datos, podemos diferenciar la videovigilancia, de la monitorización, entendiéndose por esta última la reproducción de imágenes en tiempo real, y de las que no se guarda copia, no siendo susceptibles de tratamiento o utilización, por lo que no entran dentro del ámbito de la protección de datos. Por el contrario, la videovigilancia tanto en lugares cerrados públicos, como en lugares privados, de la cual se obtiene grabación y es susceptible de tratamiento, sí entraría dentro del ámbito de la LOPD, incidiendo parte de la doctrina, como hemos adelantado, que la video-vigilancia es un medio invasivo y por tanto deben concurrir condiciones tasadas que legitimen su asunción y definan los principios y garantías que deben aplicarse. La evidencia en la propia ley que regula la video-vigilancia en el ámbito privado carece de una base armonizada y rigurosa, en donde se establezcan y legitimen los supuestos de instalación, y en donde se determinen las garantías de utilización conforme al mandato constitucional, se encuentra en la propia LO 4/1997, que en su Disposición adicional Novena, matiza que "el Gobierno elaborará, en el plazo de un año, la normativa correspondiente para adaptar los principios inspiradores de la presente Ley al ámbito de la seguridad privada", sin que hasta el momento, se haya creado normativa alguna previéndose, que en el inminente reglamento de seguridad privada que desarrollara la nueva ley de seguridad privada, pueda dilucidarse algo al respecto.

Esta inconcreción de la norma no quiere decir que la instalación uso y mantenimiento de la video-vigilancia a manos de la seguridad privada no

se someta a control, nada más lejos de la realidad, ya que la instalación de sistemas de videocámaras con fines de seguridad privada requiere la contratación de los servicios de empresas de seguridad debidamente autorizadas por el Ministerio del Interior, caracterizándose a su vez la naturaleza de la seguridad privada, de una subordinación absoluta ante las fuerzas y cuerpos de seguridad, donde la actividad y uso de video-vigilancia se somete a estrictos controles por parte de estos, determinándose mediante una serie de autorizaciones, que empresas estarán en condiciones de facilitar y ofrecer tales servicios y que personal técnico y profesional será el encargado de mantener y ejecutar los mismos, habida cuenta de la necesidad de mantener informada a las autoridades, de tales instalaciones así como los estandarizados protocolos de aviso y acuda al respecto ante cualquier alarma.

También cabe decir que la propia LOPD se encarga de ofrecer a su vez la garantía de protección jurídica al respecto de las instalaciones de video-vigilancia en ámbito privado, en donde no solo se obliga la notificación de la creación de ficheros de video-vigilancia, si la empresa de seguridad únicamente se encargó de la instalación, siendo en este caso responsabilidad del fichero la empresa o entidad que ordeno la instalación, o en el caso de que la empresa privada instaladora a su vez sea quien se ocupe de visualizar las imágenes mediante su personal de seguridad privada, al existir grabación de imágenes[5], será necesario formalizar un contrato de acceso a los datos por cuenta de terceros descrito y regulado en el artículo 12 de la LOPD y del deber de colocar, en las zonas video-vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y tener a disposición de los interesados, impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

Otros supuestos de instalación de videocámaras por la seguridad privada se someterán conforme al artículo 5.1 de la Ley 23/1992 de 30 de julio, de Seguridad Privada, donde esta se encuentra facultada para prestar entre otros, el servicio de "Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad". Estas Instalaciones estarán igualmente sometidos con carácter general a lo establecido en la LOPD y a

la instrucción 1/2006, contando con particularidades propias cuando afecte a la video-vigilancia dispuesta en Bancos, Cajas de Ahorro y demás entidades de crédito, y la que tenga por finalidad controlar el acceso a los casinos o salas de bingo, a los que se le aplicara la Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, mientras que la instrucción 1/1996, dispone las particularidades sobre los ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios. Todas estas "especialidades" estarán igualmente sujetas a lo previsto en Real Decreto 2364/1994 por el que se aprueba el Reglamento de Seguridad Privada, o la que afecte a controles de acceso a los edificios cuando comporte la toma de imágenes en que resulta aplicable la Instrucción. Como vemos, el corpus legal sobre la videovigilancia es extenso y en ocasiones difícil de acotar dadas las múltiples modalidades del servicio. La nueva Ley 5/2014, de 4 de abril, de Seguridad Privada ha introducido cambios sustanciales en materia de videovigilancia y protección de datos regulando en un artículo específico, concretamente en su art 42, sobre los Servicios de videovigilancia y que articula la novedad de posibilitar el uso de seguridad privada, incluso en espacios públicos, anteriormente materia exclusiva de las fuerzas y cuerpos de seguridad.

Artículo 42 Servicios de videovigilancia

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas. Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales. No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

Igualmente reviste especial trascendencia respecto a la protección de datos el art 15 de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

Artículo 15 Acceso a la información por las Fuerzas y Cuerpos de Seguridad

1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que permitan la comprobación de

las informaciones en tiempo real cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

También la nueva ley de seguridad privada se ocupa de las imágenes y videograbaciones que pudieren realizar los Detectives Privados como miembros de la seguridad privada, y regulados en el art 49 de la Ley 5/2014, que refiere entre otros aspectos que las investigaciones privadas tendrán carácter reservado y los datos obtenidos a través de las mismas solo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales introduciendo a su vez el citado artículo 49, limitaciones como el que no aparezcan en su informe, los datos de la persona física investigada que no sean necesarios para el objeto de los investigado, sobre todo cuando sean datos especialmente protegidos y el deber de conservación de estos informes así como imágenes y sonidos durante un plazo mínimo de tres años.

Como hemos descrito, el uso de videovigilancia tanto por las fuerzas y cuerpos de seguridad como el que puede realizar la seguridad privada, se encuentra regulado en un extenso cuerpo legal que fundamenta ambas atribuciones, con la salvedad y excepción que supone la vaguedad de una norma que reglamente los distintas naturalezas que posibilita la Seguridad Privada y que dado su continua asunción de parcelas hasta hace bien poco de titularidad pública, podría suponer un vacío legal que invalidara su desarrollo. Pero la cuestión es no de forma y si más bien de fondo, en el sentido que es necesario que la video-vigilancia, indistintamente desde su

parcela de competencias pública o privada, cumpla su objetivo ofreciendo un servicio a la ciudadanía que fundamente su actuación, dado que en ocasiones esta puede colisionar con derechos fundamentales especialmente protegidos. Con ese objeto, pasamos a describir en el siguiente epígrafe, la idoneidad y el encaje probatorio que la video-vigilancia obtiene ante los tribunales.

5. IDONEIDAD Y ENCAJE LEGAL DE LA VIDEO-VIGILANCIA COMO VALOR PROBATORIO

La actual Ley de Enjuiciamiento Criminal (LECrim.) no contiene referencias a la utilización de la videovigilancia como medio o diligencia de investigación de los hechos criminales y de sus autores, ni tampoco como medio de prueba, considerándose esta omisión en el anteproyecto de la nueva LECrim un desfase entre las nuevas tecnologías de averiguación del delito y la norma decimonónica. Aun así, la redacción del anteproyecto sigue quedándose parca respecto a las capacidades y posibilidades que suscita la toma de imagen al incorporar "nuevas medidas de investigación tecnológica" que como indicamos circunscribe su espectro a la investigación criminal ex proceso, esto es las ordenadas con un objetivo dentro de una investigación concreta, para la obtención de fuentes de prueba para el proceso, aunque si bien es común, que las grabaciones ajenas de origen extraprocesal, puedan servir igualmente como elemento de convicción en un particular proceso a tenor del tribunal. En este sentido la ausencia de previsión normativa expresa, no supone impedimento de relevancia para su admisibilidad procesal, siendo suplido por la jurisprudencia de nuestros tribunales.

En el caso que las grabaciones extraprocesales que puedan ser incorporadas a la causa, se deberá atenderse a la norma específica que faculto la disposición de esa cámara para darle validez en el proceso penal según ETXEBERRIA (2011) , como por ejemplo la propia ley de videovigilancia, pero al legislador, no le basta justificar la idoneidad de la utilización de la video-vigilancia en eventos públicos o privados a no resultar suficiente con acudir a la descripción de las finalidades genéricas

que se describen en el art 1.1 de la propia Ley 4/1997 siendo tales el *"contribución a asegurar la convivencia ciudadana, o la erradicación de la violencia o la de prevenir la comisión de delitos, faltas o infracciones relacionadas con la seguridad pública*". Cita la norma, que deberá existir un riesgo razonable para la seguridad ciudadana y/o un riesgo concreto para la utilización de video-vigilancia, según se utilicen indistintamente como video-vigilancia fija o video-vigilancia móvil, valorándose especialmente la proporcionalidad de la medida con la finalidad perseguida mediante un uso adecuado que permita efectivamente alcanzar la finalidad prevista. Aun con esta premisa, la grabación de imágenes por parte de las fuerzas y cuerpos de seguridad es práctica habitual como medio de investigación y generalmente admitida por la jurisprudencia, siempre y cuando se respeten los requisitos de proporcionalidad, idoneidad e intervención mínima.

La utilización de las videocámaras requiere superar el "test de la proporcionalidad" tanto desde la perspectiva de la idoneidad, como de la intervención mínima, establecidas en la propia norma según se desprende del art 6.2 al concretar que "la idoneidad determinará 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". En cuanto a la intervención mínima, el art 6.2 apartado 3 "exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara del derecho al honor, a la propia imagen y a la intimidad de las personas". En todos los casos se deberá establecer 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". Respecto de la idoneidad, y según Arzoz (2010), "La utilización de las videocámaras por las Fuerzas y Cuerpos de Seguridad constituye una medida adecuada para la consecución del fin perseguido, la prevención de delitos, faltas e infracciones relacionadas con la seguridad ciudadana en un lugar determinado claramente definido". *Respecto a la intervención mínima, insiste el mismo afirmando que, se ven satisfechos los requisitos de intervención como pudiera ser su utilización en detrimento de una mayor presencia policial.* Respecto al criterio de proporcionalidad en sentido estricto, la STC 207/1996 establece

una serie sobre el denominado *test de proporcionalidad*, manifestando que "[…] para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto "juicio de proporcional en sentido estricto", matizando que habrá que valorar si se cumple en cada caso concreto una proporcionalidad entre los derechos afectados y el beneficio público, si bien en general puede afirmarse que existe dicha proporcionalidad, dados los límites impuestos en la utilización de la videovigilancia y las garantías (legales, procedimentales y jurisdiccionales) establecidas legalmente para los ciudadanos (Arzoz 2010), según se han mencionado anteriormente y se especifican ahora de forma más pormenorizada:

A) la videovigilancia exige demostrar la existencia de un riesgo razonable para la seguridad ciudadana (cámaras fijas) o de un peligro concreto (cámaras móviles) (art. 6. 4);

B) debe grabarse un lugar público concreto, determinado en la autorización (art. 3. 4 LOV) y se prohíbe la grabación en el interior de las viviendas, salvo consentimiento del titular o autorización judicial (art. 6. 5);

C) se prohíbe el uso de videocámaras "cuando afecte de forma directa y grave a la intimidad de las personas", tampoco pueden grabarse conversaciones estrictamente privadas (art. 6. 5);

D) se necesita una autorización previa (salvo casos excepcionales de urgencia máxima y videocámaras móviles), con una vigencia máxima de un año por una autoridad especial independiente (art. 3, apartados 2, 3 y 4);

E) existe una restricción temporal para la conservación de las grabaciones (art. 7 y 8. 1);

F) una prohibición de la cesión o copia de las imágenes y sonidos, salvo en los supuestos del art. 8. 1 (art. 8. 3);

G) se exige la información a los ciudadanos de la existencia -aunque no del emplazamiento- y de la identificación de la autoridad responsable de las videocámaras (art. 9. 1 LOV). Además la autoridad competente para autorizar las videocámaras fijas creará un registro de las mismas (DA 2.ª);

H) y finalmente, toda persona interesada podrá ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura (art. 9. 2).

En lo que concierne al valor probatorio de la prueba video-grafica, este consiste en la captación de imágenes que determinen y configuren el iter criminis del delito, permitiendo si cabe, identificar al autor del hecho delictivo o de las personas sospechosas de realizarlo, recogidos mediante sistemas de grabación videográfica o de "otra índole" documentadas en soporte videográfico. Estas imágenes suponen hechos de interés para la investigación de infracciones penales, siendo también posible su utilización para asegurar la convivencia ciudadana, la erradicación de la violencia, la utilización pacífica de las vías y espacios públicos, así como la prevención de comisión de delitos, faltas e infracciones relacionadas con la seguridad pública, siendo válida por tanto la toma de imágenes de sospechosos de manera velada o subrepticia en los momentos en los que se supone fundadamente que se está cometiendo un hecho delictivo, pues ningún derecho queda vulnerado en estos casos al considerarse imágenes captadas sin estar previstas, por operar la casualidad de producirse donde se usan cámaras que filman lo que por azar ocurre delante de ellas, sobre todo, cuando acaba de empezar a ocurrir cualquier hecho a tenor de las flagrantes imágenes, valorándose sin apreciar por ello, infracción alguna de derecho fundamental, que pudiera declarar nulo el resultado probatorio obtenido, permitiendo al órgano juzgador probar mediante el visionado de las imágenes encartadas en el proceso penal, de una manera fiable y elocuente, toda la visión del iter delictivo que pudiera escapar a los juicios de la objetividad en la declaración de cualquier sujeto incurso en la misma, (entre otras sentencias; STS 23 febrero 2001 -EDJ 2001/3198- y STS 8 abril 2002-EDJ 2002/9872).

También pueden tener relevancia procesal otras grabaciones cuyo origen no está motivado por necesidades de vigilancia o prevención, y que

nuestros tribunales han venido admitiendo como prueba, por ejemplo las videograbaciones realizadas por medios de comunicación social en sus tareas informativas o de entretenimiento (STS 4/2005, de 19 de enero) o las grabaciones procedentes de particulares[6], aunque adquieran la calidad procesal de prueba documental carácter complementario, según la STS 7/2001, de 19 de enero, más recientemente la STS 597/2010, de 2 de junio, respecto del testimonio del sujeto que controla la filmación y ello porque, en definitiva, la filmación no es sino una técnica que permite `transferir´ las percepciones sensoriales a un instrumento mecánico que complementa y toma constancia de lo que sucede ante los que en su día disponen como testigos".

El "juicio de idoneidad" que supone la ayuda de la imagen filmada a la hora de procurar la identificación del autor, señala que la "captación y difusión de la imagen del sujeto sólo será admisible cuando la propia -y previa- conducta de aquel o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puedan colisionar con aquel" (STC 99/1994, de 11 abril) entendiendo la jurisprudencia, para su valoración -como auténtica la prueba documental en soporte audiovisual- el Tribunal debe practicar su visionado en el juicio oral, y contrastarla para aumentar la convicción, con la declaración testifical de los agentes que la obtuvieron y a su vez perfeccionando esa convicción aludida, la que proporciona la comparación de la imagen grabada por la filmación y el imputado que el tribunal tiene delante, por el propio reconocimiento ratificado en el plenario realizado por las fuerzas y cuerpos de seguridad y en caso necesario por prueba pericial antropométrica que analice los rasgos fisionómicos del autor según fotograma indubitado extraído de la grabación del hecho con los del propio acusado (entre otras; STS 27 enero 2001 -EDJ 2001/62; STS 28 septiembre 2001 -EDJ 2001/33627; 23 febrero 2001 -EDJ 2001/3198; 8 abril 2002 -EDJ 2002/9872; y 2 julio 2004 -EDJ 2004/82753).

El personal de la seguridad pública que hubiere procedido a tomar las imágenes o sonidos a incluir en las diligencias, deberán ponerlas a disposición de la Autoridad judicial en soporte original y en el menor tiempo posible, que no podrá superar las 72 horas. De modo que si no se

puede terminar la confección del atestado en ese plazo, se entregará la grabación a la vez que se pone en conocimiento verbal del Juez o del Ministerio fiscal deberá especificar las características técnicas de las cámaras empleadas y del soporte, debiendo ser el material objeto de grabación, marcado y precintado dejando constancia de la identidad de los funcionarios actuantes. Las demás grabaciones, a salvo las que se envíen para sancionar infracciones a la Autoridad administrativa competente, se destruirán en el plazo de un mes

Por lo tanto, debemos considerar que respecto a su valor procesal, la grabaciones no suponen prueba distinta a que pudiera suponer una declaración que se ampara en la percepción visual, en tanto que la jurisprudencia considera que la grabación no hace otra cosa que perpetuar la percepción que pudieran tener una o varias personas, entendiendo la jurisprudencia, que es legal la actuación basada en la imagen videográfica en los casos de investigación criminal y en los casos que exista razonable riesgo para la seguridad ciudadana o peligro concreto, conforme a derecho según la LO 4/1997 y el art. 11, letra g) y h), de la LOFCS 2/1986, de 13 de marzo, art. 2 del RD 596/1999, de 16 de abril, así como STS de 5 de mayo de 1997.

Una vez descrita muy brevemente la consideración que generalmente y de modo pacífico aluden los tribunales respecto a la valoración de la prueba video-grafica, observemos en el siguiente epígrafe, la valoración de la imagen como derecho fundamental al ser el principal encartado en colisión con otros derechos que pudiere salvaguardar la fundamentación del uso de la video-vigilancia.

6. LA IMAGEN PERSONAL TOMADA COMO DATO Y ESTE COMO DERECHO PERSONAL

A finales del siglo pasado, el tratamiento informático de la imagen[7] requería mucha capacidad y equipos informáticos potentes. Hoy esta capacidad ha variado radicalmente en donde cualquier persona tiene a su alcance un equipo exento de dificultad técnica, capad de reproducir y

grabar sonido e imagen a una calidad óptima, constituyendo si su uso no es el correcto, una potencial fuente lesiva de derechos y libertades, mientras que la regulación jurídica al efecto, no avanza con la misma celeridad de la tecnología siendo no pocas las lagunas jurídicas en relación a la toma de imagen o a la determinación de esta como dato, que los tribunales han venido tratando de solapar, como hemos visto, mediante sentencias al efecto. El Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su art. 5 f) identifica como dato de carácter personal a "cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". Y que aunque hace referencia concreta a lo "fotográfico y acústico", tales elementos constituyen la base de la imagen tomada mediante grabación, al componerse estos de sucesivos fotogramas y redundando en que lo relevante no es el medio y si el objeto de identificación y posibilidad de esta, no siendo ajena a la definición por tanto, la obtenida mediante videograbación, y definidos en el art. 3 de la Ley Orgánica 15/1999 como "Todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso".

En este sentido, la Directiva 95/46/CE Considera que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, tienen el tratamiento legal de dato, así se deduce de los Considerandos 14 y 15, mientras que en el considerando 16, matiza, que no estará comprendido como tal, los que se efectúan con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal. Con intención de desarrollar esta exclusión y dotar de una base jurídica al exponencial uso de la video-vigilancia en el ámbito público, fue sancionada mediante ley orgánica la Ley 4/1997 al afectar a diversos derechos fundaméntales, entendiendo la jurisprudencia[8], que se muestran afectados los derechos personales al dilucidar que la imagen de cada uno, es un dato personal que requiere protección aun considerando este, como un derecho no absoluto y que puede ser franqueable, según su proporcionalidad en colisión con otros

derechos fundamentales(STC 186/2000).

En este sentido, debemos partir, de que la imagen de una persona identificada o identificable constituye un dato personal, cuyo tratamiento está sujeto a la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y a la Instrucción 1/2006, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, matizando la LOPD en su artículo 2.3.e, que "Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: *Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia."* En resumen, para considerar la imagen "de cada uno" como dato y esta a su vez estar amparada por la regulación de protección de datos, es imprescindible que se pueda realizar tratamientos con ella como trasmitir o difundir, esto es formar parte de un fichero, que facilite su acceso y en donde se muestre o identifique a un sujeto sobre un soporte material cualquiera.

7. CONCLUSIONES

Si bien en España no se le ha prestado la importancia que en otros países ha supuesto la videovigilancia tales como Reino Unido o EEUU, la realidad en nuestro país nos muestra a través de las encuestas realizadas por el Centro de Investigaciones Sociológicas, durante los años 2008, 2009 y 2011, que en general se muestra un elevado nivel de apoyo al uso de cámaras, con cifras similares a las extraídas de encuestas de otros países citados, en donde esta se constituye generalmente como la primera medida preventiva de seguridad al incrementar la percepción de seguridad y protección ciudadana, considerándose una medida eficaz en la lucha contra la delincuencia. La contribución a la dispensa de seguridad que esta ofrece es palpable al comprobarse su utilidad como aportación de pruebas durante

el proceso penal es de primer orden, en cuanto tiene eficacia probatoria para formar la convicción de un tribunal sobre la existencia de un hecho o sobre la identidad de sus autores y participes coadyuvando a la persecución del delito y como herramienta disuasoria de ilícitos penales o comportamientos incívicos. También es cierto que la relación entre la prevención de los delitos mediante la tecnología monitorizada genera emotivos debates por una parte de la comunidad en donde se considera que esta invade parcelas de la intimidad personal, habiendo sido clara y concisa la jurisprudencia al considerar que habrá que valorar si se cumple en cada caso concreto una proporcionalidad entre los derechos afectados y el beneficio público, si bien en general puede afirmarse que existe dicha proporcionalidad, dados los límites impuestos en la utilización de la videovigilancia y las garantías (legales, procedimentales y jurisdiccionales) establecidas legalmente para los ciudadanos interpretando generalmente como válidas la toma de imágenes de sospechosos de manera velada o subrepticia en los momentos en los que se supone fundadamente que se está cometiendo un hecho delictivo, pues ningún derecho queda vulnerado en estos casos al considerarse imágenes captadas sin estar previstas, por operar la casualidad de producirse donde se usan cámaras que filman lo que por azar ocurre delante de ellas permitiendo al órgano juzgador probar mediante el visionado de las imágenes encartadas en el proceso penal, de una manera fiable y elocuente, toda la visión del iter delictivo que pudiera escapar a los juicios de la objetividad en la declaración de cualquier sujeto incurso en la misma. Debemos por tanto considerar que respecto a su valor procesal, las grabaciones no suponen prueba distinta a que pudiera suponer una declaración que se ampara en la percepción visual.

Respecto a la adecuación legista a las nuevas tecnologías descritas, en donde la video-grabación inteligente está tomándose en consideración por las autoridades dedicando esfuerzos en investigación y desarrollo de nuevos y más eficientes métodos de video-grabación inteligente, hemos de concluir que la legislación española actual presenta dificultades para poder responder a la misma velocidad que la tecnología ofrece sus productos, y que incluso actualmente carece de reconocimiento en concreto a la que debería tener especial incidencia como la propia ley de enjuiciamiento

criminal debiéndose reiterar la necesidad de exigir al poder ejecutivo y al poder legislativo que se haga efectiva una urgente regulación legislativa completa de este medio de investigación y prueba en el proceso penal que rellene la profunda laguna existente, adecuándose incluso a los venideros sistemas de videovigilancia inteligente, con el objeto de no posibilitar vacíos legales que puedan originar inseguridad jurídica y, por consiguiente, ineficacia.

8. REFERENCIAS

[1] Desde los acontecimientos del 11 de septiembre de 2001 en Nueva York, los acaecidos el 11 de marzo de 2004 en Madrid, el 7 de junio de 2005 en Londres y la maratón de Boston del 15 de abril de 2013 o las tragedias sucedidas en grandes reuniones de personas en actos deportivos o como la tragedia Madrid Arena del 1 de noviembre de 2012.

[2] Panóptico de Bentham. Jeremy Bentham, (filósofo británico del siglo XVIII), ideó una arquitectura carcelaria- de forma circular, con aristas interiores – el Panóptico (del latín pan-, todo; -óptico, visión), cuyo objetivo era permitir que un guardián situado en una torre, en el centro de la estructura, pudiera vigilar constante y simultáneamente a todos los presos, sin que éstos supieran en qué momento estaban siendo realmente vigilados. Bastaba con inducir a los reclusos la "sensación" de estar siendo observados para que ellos mismos se "autovigilaran" y, consiguientemente, modificaran su comportamiento.

[3] 'Eyes of Things' es un proyecto europeo de investigación de visión móvil financiado dentro del programa marco Horizonte 2020 que lidera el grupo de la Universidad de Castilla-La Mancha. La Universidad Carlos III de Madrid desarrolla un sistema inteligente que analiza en tiempo real las imágenes de las videocámaras, detecta situaciones anómalas y alerta a los agentes de seguridad más cercanos en casos de urgencia con la finalidad de mejorar la seguridad de las personas. La visualización de imágenes tridimensionales es el objetivo del Instituto Universitario de Nuevas Tecnologías de la Imagen de la Universitat Jaume I. La Universidad de

Valladolid, pretenden diseñar un sistema de videovigilancia en las grandes áreas metropolitanas mediante redes masivas de sensores. Las redes ayudarán a detectar las incidencias de la ciudad y se operarán de forma inteligente, es decir, sin necesidad de la monitorización constante de un operador humano. Investigadores de la Universidad Politécnica de Madrid han desarrollado un sistema que, utilizando varias cámaras con campos de visión solapados, estiman de manera muy precisa la posición 3D y las características espaciales de los objetos observados, algo esencial en las tareas de videovigilancia.

[4] La idoneidad sobre el uso de video-vigilancia determina que sólo podrá emplearse cuando resulte adecuado, utilizado en una situación concreta, y con el objeto del mantenimiento de la seguridad ciudadana y a su vez, para que la intervención sea mínima, se exige una ponderación, en cada caso concreto, 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.

[5] No se consideran como tales los que reproduzcan o emitan imágenes en tiempo real. Cuando el sistema de seguridad no grabe tales imágenes, sino que reproduzca y/o emita las mismas en tiempo real, dichas imágenes no darán lugar a un fichero como tal, y por lo tanto, no existirá la obligación de declarar un fichero ante el Registro de la AEPD. No obstante, ello no exime del cumplimiento del resto de obligaciones establecidas por la LOPD o en la Instrucción 1/2006, además de mantenerse la obligación de implementar carteles informativos en el lugar de captación de las imágenes, con información al usuario sobre petición y cancelación a la matriz instaladora.

[6] La aportación al proceso de las videograbaciones que tienen un origen particular está sujeta, a controles complementarios posteriores, controlando que dichas grabaciones no estén orientadas a la prevención o investigación penal y que sean ocasionales. La STS 968/1998, de 17 de julio, resuelve que no supone merma de los derechos constitucionales o garantías de los justiciables el hecho de que la filmación haya sido efectuada por un particular, "con tal que quede garantizada su integridad y autenticidad, y que sea ocasional, entendiendo por ella, la que no estando preordenada a la

prevención o investigación de hechos delictivos, pueden evidenciarlos de forma casual. Y ello, porque el principio de necesidad informador del sistema procesal penal y la aspiración del proceso penal de hacer constar la verdad material no deben ser obstaculizados por el origen circunstancial de la grabación".

[7] El Diccionario de la Real Academia Española de la Lengua define imagen como «la reproducción de los rasgos físicos de una persona sobre un soporte material cualquiera».

[8]Según la Sentencia del Tribunal Constitucional (STC 186/2000, de 10 de julio) el derecho a la intimidad y a la propia imagen, afectado por la video-vigilancia, "*no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".*

9. BIBLIOGRAFÍA

ACED FÉLEZ, E., (2003). "La protección de datos personales y la videovigilancia". Revista electrónica de la Agencia de Protección de Datos de la Comunidad de Madrid, *datospersonales.org*, nº 5.

ARZOZ SANTISTEBAN, X.,(2010).*Videovigilancia, seguridad ciudadana y derechos fundamentales*, Civitas, Madrid,

ETXEBERRIA GURIDI, J.F., (2011). La Comisión de Videovigilancia y Libertades del País Vasco. En: Videovigilancia: ámbito de aplicación y derechos fundamentales afectados, en particular la protección de los datos personales. Valencia: Tirant lo Blanch.

GOÑI SEIN, J. L., (2007). La videovigilancia empresarial y la protección de datos personales. Cizur Menor (Navarra): Civitas.

SMITH, G. J. D., (2004).Behind the screens: Examining constructions of deviance and informal practices among cctv control room operators in the uk. Surveillance and Society, 2.

ÚBEDA DE LOS COBOS, J., (2008)."Videograbación y

videoconferencia". Cuadernos de Derecho Judicial CGPJ Madrid.

VALERA, M. y VELASTIN, S.A., (2005). Intelligent distributed surveillance systems: a review. Vision, Image and Signal Processing,IEEE Proceedings, 152

CAPITULO 5

CAPITULO 5 - CONSIDERACIONES CRIMINOLÓGICAS SOBRE EL PERFIL DEL SKALTER Y EL ACECHO MEDIANTE CIBERSTALKING

1. INTRODUCCIÓN

El vocablo anglosajón stalking proviene del verbo to stalk, cuya traducción al español es el acto de seguir, acechar o perseguir sigilosamente a alguien. Su origen como delito lo encontramos en EEUU en los años 90, tras el asesinato –entre otros– de una famosa actriz por un admirador, y del continuo acoso que sufrieron celebridades del mundo del espectáculo por parte de seguidores obsesivos. La incorporación como delito en la sociedad norteamericana y anglosajona, rápidamente se extendió a multitud de países como Canadá, Australia, Dinamarca, Bélgica, Holanda, Austria, Italia o Alemania, hasta que finalmente el legislador español se ha hecho eco del mismo incorporándolo en la última reforma del Código Penal de 2015. Así pues, en el nuevo art. 172ter[196], de dicha reforma penal se proyecta en España el delito de stalking, destinado a ofrecer respuesta a conductas de indudable gravedad, penando aquel acoso o acecho obsesivo, insistente, reiterado y no consentido a otra persona que perturbe gravemente el desarrollo de su vida cotidiana.[197] Debe destacarse la relevancia de las nuevas formas de stalking

[196] "Artículo 172 ter. 1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:
1.ª La vigile, la persiga o busque su cercanía física.
2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.
3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.
4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella. (…)"

[197] Sin embargo, aunque su estudio en el ámbito de la Criminología ha sido más prolijo, desde el punto de vista estrictamente penal, España se había mostrado reticente a tipificar expresamente esta tipología delictiva, a diferencia de otros países del mundo anglosajón y en países europeos continentales como Dinamarca, Bélgica, Holanda, Austria, Alemania o Italia, donde tenía acomodo en el sistema penal con nombre propio. Garrido Genovés, V.: Amores que matan. Acoso y violencia

o ciberacoso, a que ha dado lugar la llegada de Internet, esto es, el envío de correos electrónicos constantes y repetitivos, mensajes en redes sociales de carácter amenazante, entradas en páginas web personales o profesionales para difamar o atentar contra la dignidad de su titular, o interceptación del correo electrónico.[198] Conductas que muchas veces logran quedar amparadas por el anonimato o la suplantación de personalidad que permite la red, complicando la identificación del autor, pero son tremendamente dañinas en la victima de stalking.

2. CONCEPTO DE "STALKING" Y "STALKER"

Se denomina "stalker" a la persona que lleva a cabo la conducta de stalking. El perfil del stalker, puede deberse en determinados momentos a desórdenes en la relación que le une con la víctima sentimental, de amistad, laboral, desconocidos) y la motivación de sus acciones es conseguir intimidad con la víctima, venganza, acecho, acosar y controlar a su víctima. El significado originario del término se encuentra relacionado con la caza. El verbo stalk significa perseguir o acercarse a la presa de forma sigilosa, tratando de permanecer escondido. Así pues, en la acepción de stalking objeto de este trabajo, se identificaría el cazador con el acosador y la presa con la víctima.

La doctrina a atribuido al termino variadas definiciones. Entre las cuales nosotros aquí consideramos apropiado, basándonos en Villacampa, definir el stalking como "la conducta reiterada e intencionada de persecución obsesiva respecto de una persona, su objetivo, y este seguimiento por parte del Stalker, es realizado en contra de la voluntad de la víctima en la que crea, sensación de aprensión o es lo suficientemente constante, para ser susceptible de provocarle miedo

contra las mujeres. Alzira, Algar, 2001

[198] ALONSO DE ESCAMILLA, A. *El delito de Stalking como nueva forma de acoso. Cyberstalking y nuevas realidades,* La Ley Penal, nº 105, Sección Estudios, noviembre-diciembre 2013

razonablemente".[199]

Esta conducta descrita como acción del Stalker y reacción en la victima, podríamos considerar que contiene los elementos esenciales comunes en el delito de stalking.

 Conducta reiterada e intencionada: Es fundamental para apreciar la existencia de acoso que la conducta esté constituida por concretos actos que se producen repetidamente en el tiempo. Esto se debe a que los actos de acoso, individualmente considerados, no suelen tener la suficiente gravedad como para fundamentar una respuesta de las autoridades. Existen distintas opiniones respecto al número de actos y período temporal en el que estos se deben producir para considerar la conducta constitutiva de stalking. Para Pathé y Mullen, la conducta debe consistir al menos, en diez intrusiones o comunicaciones no deseadas en un período de al menos cuatro semanas.[200] Según Magro Servet un acoso puntual, aunque haya sido de dos días o dos o tres veces no sería delito, sino que se requiere llegar al convencimiento de que hay una persistencia en el acoso y que ante la negativa o la oposición de la víctima el acosador persiste en su actitud.[201]

 Conducta de persecución obsesiva: los actos que constituyen las concretas conductas de acoso son persecutorios en tanto que se dirigen a una persona y buscan su cercanía, ya sea física, visual, directa o indirecta. Estos actos comúnmente se han asociado a conductas de acoso predatorio son: llamar por teléfono, enviar cartas, e-mails o regalos, seguir a la víctima en el exterior, así como merodear por los alrededores de su casa, conductas irrelevantes o incluso socialmente aceptadas de

---

[199] VILLACAMPA ESTIARTE, C.: *Stalking y derecho penal*. Relevancia jurídico-penal de una nueva forma de acoso, Ed. Iustel, Madrid, 2009.p 32

[200] Ibídem., pág.37.

[201] No es suficiente con la referencia a que la conducta haya de ser "insistente y reiterada" sino que se debe exigir la existencia de una estrategia sistemática de persecución, integrada por diferentes acciones dirigidas al logro de una determinada finalidad que las vincule entre ellas. Lo esencial en el stalking sería la estrategia sistemática de persecución, no las características de las acciones en que ésta se concreta. MAGRO SERVET, V.: "Los delitos de sexting (197.7) y stalking (172 ter) en la reforma del Código Penal", Ponencia de formación continuada en la Fiscalía General del Estado, 16 marzo 2015 – Ponencia. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/2%20ponencia%20Sr%20Magro%20Servet.pdf?idFile=6db6bcf5-dbe7-4e3a-bb0b-cfee027d2484

ser consideradas aisladamente o de ser queridas por su destinatario. También incluyen conductas de distinta naturaleza más graves y que podrían constituir por sí mismas delito tales como irrumpir en casa de la víctima, la formulación de amenazas, sustracción de sus bienes, difamaciones o falsas acusaciones, publicación de imágenes íntimas de la víctima, o asaltar a la víctima o retenerla.

 Conducta no deseada: La conducta no ha de ser deseada por la víctima, sino que ha de ser realizada en contra de su voluntad, una intrusión no consentida en su espacio vital. Como veremos, esa intrusión en la esfera privada de la víctima se ha visto facilitada por las nuevas tecnologías El precepto exige que la realización de la conducta típica altere gravemente el desarrollo de la vida cotidiana del sujeto pasivo. Es por este motivo que se configura como un delito contra la libertad de obrar.[202]

 Conducta susceptible de provocar miedo razonable: La conducta ha de ser percibida como amenazante o intimidatoria, produciendo de esta manera sensación temor, malestar, inquietud o angustia en la víctima que influyen negativamente en el desarrollo normal de su vida. Dicho peligro no tiene porqué llegar a materializarse ni ser concreto. Ejemplo típico que señala Gómez Rivero es el del seguimiento de la víctima, lo cual la genera un sentimiento de intranquilidad frente a un posible ataque de su acosador, pero sin saber qué clase de ataque ni de lo que este es capaz. Podría ser un ataque a su patrimonio, a su integridad física, a su vida o a su libertad sexual. Es precisamente dicho desconocimiento sobre el qué, el cómo y el cuándo lo que genera mayor afectación al desarrollo vital de la víctima.[203]

---

[202] Se introduce un elemento negativo del tipo a modo de eximente de la punibilidad, por cuanto otro de los elementos de este delito es el "no estar legítimamente autorizado" para realizar las conductas descritas en el tipo penal, algo que conforme a la mayor parte de la doctrina resulta superfluo y sorprendente, porque no se entiende esta referencia a que alguien pudiera estar legitimado para llevar a cabo conductas de acoso.

[203] GÓMEZ RIVERO, Mª C.: "El derecho penal ante las conductas de acoso persecutorio", en MARTÍNEZ GONZÁLEZ, MªI (dir.) El acoso: tratamiento penal y procesal, Valencia, 2011, pág.31.

3. EL NUEVO DELITO DE ACECHO

Hemos de advertir que el stalking no es una conducta o problema nuevo, sino que, tal y como afirma Villacampa, es el cambio de actitud de la sociedad frente a dicho problema el que explica la criminalización de la conducta. Dicho fenómeno de criminalización se originó en Estados Unidos y se fue expandiendo a Europa a través de los países del common law.[204] La Ley Orgánica 1/2015 introdujo en el Código Penal el nuevo delito de acoso -también denominado stalking, que introduciría el matiz de acecho- dentro del capítulo dedicado a los delitos contra la libertad, tratando de regular todos aquellos supuestos en los que, sin que se haya llegado a producir la amenaza o ejecutado el acto de violencia que exige la coacción, se producen conductas reiteradas en el tiempo por medio de las cuales se menoscabe gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones, vigilancias constantes, llamadas reiteradas y otros actos de hostigamiento.

Hasta la entrada en vigor del nuevo artículo 172 ter, estas modalidades de acecho, ofrecían serias dificultades para su tipificación y en multitud de ocasiones quedaban impunes. Conductas como la persecución, la continua vigilancia o el envío masivo de mensajes o emails, de llamadas, etc, que causaban un temor y preocupación en la víctima por parte del "Stalker", no cumplían en muchos casos los requisitos para ser tipificadas como coacciones ni amenazas del 620.2 del Código Penal, al considerarse que no siempre existía una intención manifiesta de causar daño o empleo de violencia, con el fin de coartar la voluntad de la víctima acechada.

Tales conductas de acecho que se sucedían entre parejas y ex parejas[205] ofrecían

[204] De acuerdo con esta autora, los medios de comunicación, desde los años ochenta, contribuyeron significativamente a la construcción social del problema, vinculándolo al comienzo fundamentalmente a las celebridades y fans obsesionados y, a partir de los noventa, con la violencia de género. Fue la presión de las organizaciones de mujeres maltratadas y demás organizaciones pro derechos de las víctimas, junto con la ausencia de oposición la que determinó su criminalización: VILLACAMPA ESTIARTE, C.: Stalking y derecho penal. Ob cit, p.57 y ss.

[205] La lucha contra la violencia de género se verá claramente reforzada con la entrada en vigor de

igualmente dificultades para su tipificación, pues no cumplían los requisitos para ser tipificadas como coacciones ni amenazas al no existir una intención manifiesta de causar daño o empleo de violencia a fin de coartar la voluntad de la víctima. Se trata con esta nueva figura delictiva, de considerar todos aquellos supuestos, en los que, sin llegar a producirse necesariamente el anuncio explícito o no de la intención de causar algún mal (amenazas), o el empleo directo de la violencia para coartar la libertad de la víctima (coacciones), se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas, u otros actos continuos de hostigamiento. Con anterioridad a la reforma del 2015, no existía un tipo penal específico para estas conductas, que se venían castigando en algunos casos como delito de coacciones del art. 172.2, o como vejaciones leves o amenazas, ex art. 620 CP, y para los episodios más graves, casos de molestias o amenazas continuadas capaces de producir en la víctima un nivel de humillación elevado y grave, se venía aplicando el art. 173 CP, como delito contra

---

este nuevo tipo penal, en cuanto el párrafo 3 del mismo artículo prevé un agravamiento de la pena (pena de prisión de uno a dos años o trabajos en beneficio de la comunidad de sesenta a ciento veinte días) en el caso de que el stalker (acosador) lleve a cabo la conducta de acecho u hostigamiento sobre las personas a las que se refiere el apartado 2 del artículo 173, es decir, que entre sujeto activo y pasivo exista o haya existido una determinada relación de afectividad. En los casos de violencia de género es una conducta que se repite con mucha frecuencia a raíz de la separación de la pareja, viéndose la mujer acosada por su ex pareja que no acepta la ruptura de la relación y movido el hombre por un sentimiento de propiedad, recurre a la vía del acoso, persecución, vigilancia, hostigamiento, imponiendo su presencia, remitiendo mensajes o llamadas de manera insistente y constante con el fin de vencer la oposición de la víctima y retomar la relación. De éste modo, el art. 172.ter prevé un tipo agravado en su ordinal segundo si la víctima es alguna de las personas contempladas en el art. 173.2 del Código Penal "la que sea o haya sido su cónyuge o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, o sobre los descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente, o sobre los menores o personas con discapacidad necesitadas de especial protección que con él convivan o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente, o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de su convivencia familiar, así como sobre las personas que por su especial vulnerabilidad se encuentran sometidas a custodia o guarda en centros públicos o privados". En estos casos no será necesaria la denuncia de la persona agraviada. MAGRO SERVET, V. Reforma del Código Penal afectante a la violencia de género, La Ley Penal, nº 114, mayo-junio 2015

la integridad moral; si bien ninguno de estos preceptos abarcaban todo el desvalor de la acción.[206] Con este nuevo delito de acoso se pretende proteger diferentes bienes jurídicos, entre ellos la libertad de obrar como capacidad de decidir libremente, ya que con las conductas previstas en el tipo penal se afecta al proceso de formación de la voluntad de la víctima que sufre temor, intranquilidad y angustia como consecuencia del acechamiento del acosador. La redacción admite, por tanto, un concepto amplio de acoso (acción y efecto de acosar), que en interpretación literal significa perseguir, sin darle tregua ni reposo, a una persona o perseguir, apremiar, importunar a alguien con molestias o requerimiento[207].

Por otro lado, se trata de proteger la seguridad de la víctima, entendida como el derecho al sosiego y tranquilidad personal, que se puede ver afectada por conductas que limiten dicha libertad de obrar. Y, por último, estas conductas también pueden afectar a otros bienes jurídicos como el honor, la integridad moral o la intimidad.[208]

Pero su regulación no sólo está dirigida al ámbito de la violencia machista, sino que el delito de stalking va más allá, pudiendo ser sujeto activo y pasivo tanto hombre como mujer, incluso personas del mismo sexo, siempre que la conducta obsesiva

---

[206] Un sector importante de la doctrina criminológica, entendía insuficiente la derivación de esta clase de conductas a los tipos penales ya existentes, reclamando su regulación como delito autónomo. La mayor parte de las conductas hoy entendidas como acoso, encontraban un relativo acomodo en el delito de coacciones (art. 171 CP), de tal modo que "se ha erigido de facto en el delito al que la jurisprudencia española reconduce la mayor parte de supuestos de stalking" plasmándose sobre el papel en el último elenco punitivo y, llevado a la práctica por primera vez en un tribunal en la SJI de Tudela, de 23 marzo 2016. VILLACAMPA ESTIARTE, C.: "La respuesta jurídico-penal frente al stalking en España: presente y futuro", en *ReCrim*, 2010.

[207] Sin embargo, la doctrina ha definido diversas modalidades de acoso: moral y el acoso psicológico. Aquél busca humillar o envilecer a la víctima, mientras que éste no busca producir en la víctima dichos sentimientos, sino los de preocupación, temor, inseguridad o desasosiego, entre otros. Es con el acoso psicológico con el que parecen identificarse muchas de las conductas del stalker, mientras que el acoso moral perfectamente puede ubicarse entre los delitos contra la integridad moral. En realidad, el stalking parece encajar en la mayor parte de sus modalidades comisivas con el término de acecho, que en interpretación literal significa ". DE LA CUESTA ARZAMENDI, J.L. Y MAYORDOMO RODRIGO, V.: "Acoso y Derecho penal", en Eguzkilore, Nº 25, 2011. p22.

[208] En los casos más graves, podrá además darse múltiples y variadas relaciones concursales del stalking viéndose afectados otros bienes jurídicos como la libertad, la vida, el honor o la intimidad, entre otros. DOVAL PAÍS, A. Nuevos límites penales para la autonomía individual y la intimidad, Thomson Reuters Aranzadi

del stalker reúna los requisitos del tipo penal.

4. EL BIEN JURÍDICO PROTEGIDO

El bien jurídico principalmente afectado por el stalking es la libertad (en particular sobre la libertad de obrar), aunque también pueden verse afectados otros bienes jurídicos como el honor, la integridad moral o la intimidad, en función de los actos en que se concrete el acoso. El acoso es una acción, como reza la exposición de motivos, en la que sin llegar a producirse necesariamente el anuncio explícito de causar algún mal (amenazas) o el empleo directo de violencia para coartar la libertad de la víctima (coacciones), se realizan conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas, u otros actos continuos de hostigamiento. También debemos considerar como bien jurídico protegido la seguridad, esto es, el derecho al sosiego y a la tranquilidad personal. Sin embargo, solo adquirirán relevancia penal las conductas que limiten la libertad de obrar del sujeto pasivo, sin que sea punible el mero sentimiento de temor o molestia. No obstante, trayendo a colación la resolución de la primera sentencia citada de stalking, el bien jurídico protegido, es la libertad de obrar, entendida como la capacidad de decidir libremente.[209] Las conductas de stalking afectan al proceso de formación de la voluntad de la víctima en tanto que la sensación de temor e intranquilidad o angustia que produce el repetido

[209] SJI Tudela (Provincia de Navarra), Procedimiento, diligencias urgentes nº 0000260/2016 de 23 de marzo 2016 (ARP 2016, 215) La sentencia, en suma, nos indica que estamos ante un delito pluriofensivo, lo que de base dificulta establecer en qué momento se vulnera un determinado bien jurídico encontrándonos realmente ante una conducta antijurídica punible y no un mero acto inocuo. El precepto presenta una defectuosa técnica jurídica y falta de precisión en detrimento de la seguridad jurídica predicada por el principio de legalidad en su vertiente de taxatividad (lex stricta). SERGIO CÁMARA, A. La primera condena en España por acecho o stalking. Revista Unir junio 2016. Documento en línea.
http://www.unir.net/derecho/revista/noticias/la-primera-condena-en-espana-por-acecho-o-stalking/549201499291/

acechamiento por parte del acosador, le lleva a cambiar sus hábitos, sus horarios, sus lugares de paso, sus números de teléfono, cuentas de correo electrónico e incluso de lugar de residencia y trabajo.[210]

5. CONDUCTA TÍPICA

Tal como se desprende del precepto, se castiga el hecho de acosar, llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas descritas. Se trata por tanto de un delito común que puede cometerse por cualquier persona. Si hay relación conyugal o análoga, en los términos que establece el art. 173.2 CP, tendremos una modalidad de stalking agravada que encaja dentro de la denominada violencia de género[211] y aunque originariamente se trata de un delito que se introduce pensando en el ámbito de la violencia de género, no se exigen características específicas del sujeto activo y pasivo, incluyéndose como sujetos activos tanto hombres como mujeres, siendo la relación entre ellos irrelevante, independientemente que, de menare acertada por el legislador, se establezca un subtipo agravado para cuando el acoso se produzca en el ámbito familiar.

Es decir, para acotar unívocamente la siguiente conducta típica[212]:

---

[210] Se trata de una acepción restringida del término, puesto que algunos autores han identificado la libertad de obrar en un sentido más amplio que abarca tres dimensiones "libertad de formación de la voluntad, libertad de decisión de la voluntad/libertad de decidir, libertad de ejecución de la voluntad/libertad de obrar" VILLACAMPA ESTIARTE, C.: "La respuesta jurídico-penal frente al stalking en España: presente y futuro", ob cit p41.

[211] MAGRO SERVET, V.: "Los delitos de sexting (197.7) y stalking (172 ter) en la reforma del Código Penal", Ponencia de formación continuada en la Fiscalía General del Estado, 16 marzo 2015. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/2%20ponencia%20Sr%20Magro%20Servet.pdf?idFile=6db6bcf5-dbe7-4e3a-bb0b-cfee027d2484

[212] Existe un apartado 4. a la descripción típica que trasladamos aquí. 4.El apartado cuarto del precepto establece la necesidad de denuncia de la persona agraviada o de su representante legal como requisito de procedibilidad, pero no se requerirá denuncia previa cuando el ofendido sea alguna de las personas a las que se refiere el art. 173.2 CP (el cónyuge del autor, o la persona que

1, Se exigirá que nos hallemos ante un patrón de conducta, descartando actos aislados.

2, Se exigirá igualmente una estrategia sistemática de persecución, integrada por diferentes acciones dirigidas al logro de una determinada finalidad que las vincule entre ellas.

3. Se exigirá que la conducta típica altere gravemente el desarrollo de la vida cotidiana del sujeto pasivo.

Entre las notas definitorias del stalking podemos encontrar, por tanto:

a) la existencia de actos de acoso de distinta naturaleza de forma continuada, insistente y reiterada.

b) falta de consentimiento de la víctima.

c) alteración grave del desarrollo de la vida cotidiana de la víctima

Mientras que para ser punible, el acoso deberá realizarse a través de alguna de estas cuatro modalidades de conducta_

1. Vigilar, perseguir o buscar la cercanía física de la víctima, incluyéndose conductas tanto de proximidad física como de observación a distancia y/o a través de dispositivos electrónicos de seguimiento y/o mediante cámaras de vídeo vigilancia etc.

2. Establecer o intentar establecer contacto con la víctima a través de cualquier medio de comunicación o por medio de terceras personas, incluyéndose, tanto la tentativa de contacto como el propio contacto.

3. El uso indebido de sus datos personales para la adquisición de productos o mercancías, el contrato de servicios o hacer que terceras personas se

esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia; sus descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente; o los menores o personas con discapacidad necesitadas de especial protección que con él convivan o se hallen sujetos a su potestad o tutela …).

pongan en contacto con la víctima, manifestándose este puesto, aquellos casos en los que el sujeto activo publica un anuncio en Internet ofreciendo algún servicio que provoca que la víctima reciba múltiples llamadas.

4. Atentar contra la libertad o el patrimonio de la víctima o de alguna persona próxima a la víctima.[213]

6. CONSIDERACIONES CRIMINOLÓGICAS SOBRE EL PERFIL DEL SKALTER

Los Stalkers son conducidos a menudo por la venganza, el odio, la cólera, los celos, y la obsesión Si bien un Stalkers puede estar motivado por algunos de estos mismos sentimientos, a menudo el acoso es impulsado por el deseo de asustar o avergonzar a la víctima o de llamar su atención. La actitud del Skalter a través de los medios electrónicos, denominada cyberstalking casi siempre se caracteriza porque este, persigue implacablemente a su víctima en línea usando diferentes redes, comunicaciones digitales u herramientas de vigilancia en red. El stalking entre conocidos ha sido siempre el más habitual,[214] y dentro de ellos, el surgido entre ex parejas, con el exponencial aumento del uso de las nuevas tecnologías de la

[213] No especificándose en la primera sentencia aludida, qué clase de atentado contra la libertad o patrimonio. Es decir, si se trata de los ya específicamente tipificados en el Código Penal, o bien si se incluyen también conductas no tipificadas como delito. Según la sentencia, alguna parte de la doctrina defiende la inclusión de la amenaza de atentado a la libertad, y de la amenaza y atentado contra la vida y la integridad física. Pese a que estos delitos ya se encuentran tipificados en el correspondiente delito de amenazas o coacciones, también es cierto que lo están en los correspondientes delitos contra el patrimonio y contra la libertad El juez explica que el bien jurídico protegido es la libertad de obrar, entendida como la capacidad de decidir libremente. Las conductas de stalking afectan al proceso de formación de la voluntad de la víctima en tanto que la sensación de temor e intranquilidad o angustia que produce el repetido acechamiento por parte del acosador, le lleva a cambiar sus hábitos, sus horarios, sus lugares de paso, sus números de teléfono, cuentas de correo electrónico e incluso de lugar de residencia y trabajo. Asimismo, añade el magistrado, se protege también el bien jurídico de la seguridad, esto es, el derecho al sosiego y a la tranquilidad personal. SJI Tudela (Provincia de Navarra), Procedimiento, diligencias urgentes nº 0000260/2016 de 23 de marzo 2016 (ARP 2016, 215)

[214] GÓMEZ RIVERO, MªC.: El derecho penal ante las conductas de acoso persecutorio…, op. cit., pág.43.

comunicación y la creciente costumbre de compartir y exponer nuestras vivencias, experiencias, gustos y, en general, nuestros datos personales en Internet, puede aumentar el caso de acoso entre desconocidos. El anonimato que ofrece la red permite a todo individuo acceder a dichos datos y contactar con otros sin que sea identificado. Estos dos factores, son el perfecto caldo de cultivo para que surja el acoso[215]. También el Stalker puede incluir en su conducta de acoso, algún tipo de acecho fuera de línea. Esta conducta fuera de línea lo convierte en una situación más grave ya que puede conducir fácilmente a un contacto físico peligroso, si se conoce la ubicación de la víctima. Mediante el cyberstalker el acosador sigue a su víctima en foros, grupos y redes sociales, y publican mentiras y mensajes de odio, o transmiten información errónea sobre la víctima

6.1. ¿Qué hace el cyberstalkers cuando acecha o acosan a alguien?

La intención del cyberstalker es causar miedo, castigar o lastimar a la víctima. El acosador puede publicar comentarios destinados a causar angustia a la víctima, o hacer que sean objeto de acoso por parte de otros. Pueden enviar una corriente constante de correos electrónicos y mensajes a su víctima o a los compañeros de trabajo de esta, a sus amigos o a su familia. Pueden presentarse como la víctima y enviar comentarios ofensivos o enviar mensajes ofensivos en su nombre. Pueden enviar comunicaciones odiosas o provocativas al jefe de la víctima, a su familia o a otra persona significativa (en su propio nombre o haciéndose pasar como víctima). A menudo, la computadora de la víctima es hackeada o sus cuentas de correo electrónico o de redes sociales son interrumpidas por el cyberstalker y se asumen por completo, o la contraseña se cambia y la víctima es bloqueada de sus propias cuentas. La víctima puede estar registrada para spam, sitios pornográficos u ofertas

[215] GARCÍA GONZÁLEZ, J.: Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, Tirant lo Blanch, Valencia, 2010, pág.10.

cuestionables. Si tienen imágenes reales sexualmente explícitas o desnudas de sus víctimas (generalmente de una relación romántica fallida entre el acosador / acosador y la víctima), pueden crear sitios Web que publican las imágenes y anuncian el sitio a los amigos y familiares de la víctima, o suministrarlos a sitios de porno amateur, para la exhibición pública.

El propio medio en el que se desarrolla, hace que el cyberstalking presente unas características propias que no se encuentran en la forma de stalking tradicional. Estas características son[216]:

Invisibilidad: El anonimato que proporciona Internet hace que el agresor actúe con sensación de impunidad. Actuar desde el anonimato en una realidad sobre la que se tiene capacidad de influir y modificar, otorga una grata sensación de poder y libertad. El hecho de saberse anónimo desinhibe: siendo capaces de hacer o decir cosas que no tendrían lugar fuera de la red.

Ausencia de contacto directo con la víctima: El acosador tiene menor percepción del daño causado y difícilmente podrá empatizar con la víctima. Al mismo tiempo, no obstante, la ausencia de contacto directo con la víctima, Internet provoca una intimidad acelerada: en general, las relaciones se abren más, y con mayor intensidad e intimidad cuando se establecen online.

Desamparo legal: Ausencia de mecanismos rápidos y efectivos de protección para la víctima. Aunque se cierre la web, inmediatamente se puede abrir otra.

Invade ámbitos de privacidad: aparentemente seguros como el hogar familiar, desarrollando un sentimiento de desprotección total en la víctima.

Es un acoso público: se abre a más personas rápidamente y es fácil para el cyberacosador invitar a otras personas a participar en el cyberacoso.

Facilidad de difusión, reproducción y accesibilidad: Internet está siempre disponible, es constante y carece de horarios. Lo único que necesita el cyberstalker

[216] GARCÍA GONZÁLEZ, J.: Ciberacoso: la tutela penal de la intimidad…, op. cit., pág.17 y ss (referido a Ciberbullying pero extrapolable al cyberstalking).

es un ordenador o smarthphone con acceso a Internet.

Además, hemos de tener en cuenta que el cyberstalking podría convertirse en stalking, si su víctima decide cancelar o inhibirse de la red, dada la facilidad de acceso del stalker a nuestros datos privados como el teléfono, lugar de trabajo, o domicilio.[217]

6.2. ¿Quién es el stalker típico?

La mayoría de las víctimas del stalking conocen a sus acosadores en la vida real. Algunas de las características más comunes de su perfil criminal serían las siguientes: la mayor parte de los acosadores (entre un 70-80%) son de sexo masculino[218], si bien también se ha investigado el perfil de la mujer acosadora[219]. Es habitual que hayan terminado el bachillerato o tengan educación universitaria y sean significativamente más inteligentes que otras tipologías de delincuentes y no aparece un porcentaje que descollé en ningún grupo étnico o racial. Pueden ser compañeros de trabajo, ex cónyuges, erotomaniacos, alguien con rencor o interesado en la misma persona que la víctima, o pretendientes frustrados cuyos avances fueron ignorados o rechazados especialmente cuando la relación no progresa según lo anticipado por el stalker. La media de la edad de los acosadores tiende a ser mayor que la de otros delincuentes, encontrándose entre los 35 y 40 años de media.[220]. También podrían ser fans o groupies, especialmente cuando se trata de una ciber-celebridad o un bloguero influyente digital conocido. La

[217] M.GREGORY, T.: "Cyberstalking: Dangers on the Information Surperhighway"…, op. cit., 2001, pág.1.
[218] MELOY, J.R.: "Stalking: An old behavior, a new crime", en *Psychiatric Clinics of North America*, Nº22, 1999.
[219] MELOY, J.R., & BOYD, C.: "Female stalkers and their victims", en Journal of the American Academy of Psychiatry and the Law, Nº 31, 2003.y mas recientemente MELOY, J.R., MOHANDIE, K., & GREEN, M.: "The Female Stalker", en Behavioral Sciences and the Law, 2011.
[220] MULLEN, P., PATHE, M., & PURCELL, R.: "Study of stalkers", en American Journal Psychiatry, Nº 156, 1999.

venganza, el odio, y el romance son los motivos más frecuentes para el agresor mediante cyberstalking. Asimismo, es frecuente encontrar fracasos sentimentales o relaciones fallidas como característica común entre los acosadores[221] Es bastante común que la situación de acoso se produzca inmediatamente después de una ruptura sentimental, separación o divorcio, así como que sea realizada por personas con dificultades para entablar relaciones afectivas sanas y estables (Mullen et al., 1999).

7. LA CONDUCTA CRIMINÓGENA DEL STALKER COMO MATERIALIZACIÓN DE VIOLENCIA REACTIVA O VIOLENCIA INSTRUMENTAL

La violencia reactiva está relacionada con una baja resistencia a la frustración[222]. Es bastante común que la situación de acoso se produzca por personas con dificultades para entablar relaciones afectivas sanas y estable. A este respecto, está demostrado que altos niveles de dificultad y frustración pueden generar violencia reactiva cuando no van acompañados de las capacidades necesarias para superar dichas dificultades[223]. Esta agresión suele relacionarse con la existencia de un sesgo en la interpretación de las relaciones sociales que se basa en la tendencia a realizar atribuciones propias sobre el comportamiento de los demás. Tal atribución va acompañada de una carencia de habilidades para la resolución de conflictos. La falta de satisfacción de deseos o necesidades, ya sean estos básicos o no, lleva a

[221] MELOY, J.R.: "Stalking: An old behavior, a new crime", en Psychiatric Clinics of North America, Nº22, 1999.
[222] HUBBARD, J. A. DODGE, K. A., CILLESSEN, A. H. N., COIE, J. D. Y SCHWARTZ, D. (2001). The Dyadic Nature of Social Information Processing in Boys' Reactive and Proactive Aggression. Journal of Personality and Social Psychology, 80, 268-280.
[223] HUBBARD, J. A., SMITHMYER, C. M., RAMSDEN, S. R., PARKER, E. H., FLANAGAN, K. D., DEARING, K. F., RELYEA, N. ET ÁL. (2002). Observational, Physiological, and Self-Report Measures of Children's Anger: Relations to Reactive versus Proactive Aggression. Child Development, 73, 1101- 1118.

desarrollar comportamientos violentos.[224] El motivo principal de este tipo de violencia es dañar al otro individuo y se caracteriza por la carencia de funciones inhibitorias, por un autocontrol reducido, por la baja capacidad de planificación, por elevados niveles de impulsividad y por la hostilidad[225]. Mientras que, la violencia instrumental, consiste en actos intencionales, planificados y premeditados de violencia utilizados como medio para resolver conflictos, controlar el comportamiento de los demás o conseguir beneficios o recompensas. Estos beneficios son valorados por los agresores por encima del daño que puedan ocasionar a las víctimas, lo que no supone por parte del agresor una necesidad primaria de causar daño a dichas víctimas[226]. Los orígenes de la agresividad instrumental, se encuentran estrechamente relacionados con la teoría del aprendizaje social de Bandura[227]. Este tipo de violencia se relaciona con la tendencia a pensar que este tipo de agresión es una manera efectiva de obtener beneficios, por lo cual los agresores la valoran mucho y la justifican, al tiempo que ven reforzada su atribución de autoeficacia[228]. Los agresores instrumentales carecen de sentimientos de culpa o arrepentimiento, presentando además bajos niveles de empatía. [229]. La violencia instrumental se desarrolla a una edad más avanzada que la violencia reactiva[230].

A pesar de que usar esta diferenciación entre violencia reactiva e instrumental ha

[224] GARAIGORDOBIL, M. Y OÑEDERRA, J. A. (2010), La violencia entre iguales. Revisión teórica y estrategias de intervención. Madrid: Pirámide.
[225] RAINE, A., DODGE, K., LOEBER, R., GATZKE-KOPP, L., LYNAM, D., REYNOLDS, C., STOUTHAMER-LOEBER ET ÁL. (2006). The Reactive-Proactive Aggression Questionnaire: Differential Correlates of Reactive and Proactive Aggression in Adolescent Boys. Aggressive Behavior, 32, 159-171.
[226] RAMÍREZ, J. M. Y ANDREU, J. M. (2003). Aggression's Typologies. International Review of Social Psychology, 16, 125-141.
[227] BANDURA, A. (1982). Teoría del aprendizaje social. Madrid: Espasa Calpe.
[228] ANDREU, J. M. RAMÍREZ, J. M. Y RAINE, A. (2006). Un modelo dicotómico de la agresión: valoración mediante dos autoinformes (CAMA y RPQ). Psicopatología Clínica, Legal y Forense, 5, 25-42.
[229] AMOR, P. J. (2005). Personalidades violentas. Revista Crítica, 925, 24-28.
[230] CHAUX, E. (2003). Agresión reactiva, agresión instrumental y ciclo de la violencia. Revista de Estudios Sociales, 15, 47-58.

demostrado, como ya hemos expuesto recientemente, ser eficaz en el estudio de las manifestaciones violentas, y aunque son varios los autores que se han mostrado críticos con ellas, estas críticas se centran fundamentalmente en la concepción dicotómica de la violencia instrumental y la violencia reactiva, según la cual las características expuestas para cada tipo de violencia constituyen aspectos propios y exclusivos de cada una de ellas. Bushman y Anderson proponen la existencia de un solapamiento de ambos tipos de violencia[231]. Ambos tipos de violencia reactiva e instrumental se solapan, donde ambos tipos de agresividad constituyen los extremos de un continuo en el que la agresión reactiva puede adquirir progresivamente connotaciones de agresión instrumental debido a los beneficios que el acto agresivo reporta. Felson por su parte, considera que toda violencia es instrumental, ya que cuestiona que cualquier acto violento por impulsivo que este parezca, no está carente de reflexión.[232] Para este autor, las motivaciones que guían cualquier acto de agresión pueden encontrarse tanto en la violencia instrumental como en la reactiva, denominadas por Felson «agresión relacionada con las disputas», en el caso de la violencia reactiva, y «agresión predatoria» en el caso de la violencia instrumental. Atendiendo a esta dicotomía, la violencia reactiva se caracteriza, según hemos expuesto, por altos niveles de impulsividad, mientras que la violencia instrumental lo hace por una elevada capacidad de planificación y premeditación.

8. REFERENCIAS

ALONSO DE ESCAMILLA, A. (2013). El delito de Stalking como nueva forma de Acoso. Cybertalking y nuevas realidades, La Ley Penal, nº 105, Noviembre-Diciembre

[231] BUSHMAN, B. J. Y ANDERSON, C. A. (2001) Is it Time to Pull the Plug on the Hostile versus Instrumental Aggression Dichotomy? Psychological Review, 108, 273-279.
[232] FELSON, R. B. (2002). Violence and Gender. Reexamined. Washington D. C.: American Psychological Association.

AMOR, P. J. (2005). Personalidades violentas. *Revista Crítica,* 925, 24-28.

ANDREU, J. M. RAMÍREZ, J. M. Y RAINE, A. (2006). Un modelo dicotómico de la agresión: valoración mediante dos autoinformes (CAMA y RPQ). Psicopatología Clínica, Legal y Forense, 5, 25-42

BANDURA, A. (1982). Teoría del aprendizaje social. Madrid: Espasa Calpe.

BUSHMAN, B. J. Y ANDERSON, C. A. (2001) Is it Time to Pull the Plug on the Hostile versus Instrumental Aggression Dichotomy? *Psychological Review,* 108, 273-279.

CHAUX, E. (2003). Agresión reactiva, agresión instrumental y ciclo de la violencia. *Revista de Estudios Sociales,* 15, 47-58.

DE LA CUESTA ARZAMENDI, J.L. y MAYORDOMO RODRIGO, V.: (2011) "Acoso y Derecho penal", *en Eguzkilore,* Nº 25,. p22

DÍAZ LÓPEZ, J.A., (2013). El odio discriminatorio como agravante penal. Sentido y alcance del art. 22.4 CP, Civitas, Madrid.

DOVAL PAÍS, A. (2015). Nuevos límites penales para la autonomía individual y la intimidad, Thomson Reuters Aranzadi. Cizur Menor.

FELSON, R. B. (2002). Violence and Gender. Reexamined. Washington D. C.: *American Psychological Association.*

GARCÍA GONZÁLEZ, J.: (2010). Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, Tirant lo Blanch, Valencia.

GARAIGORDOBIL, M. Y OÑEDERRA, J. A. (2010), La violencia entre iguales. Revisión teórica y estrategias de intervención. Madrid: Pirámide.

GARRIDO GENOVÉS, V.: (2001). Amores que matan. Acoso y violencia contra las mujeres. Alzira, Algar.

GREGORIE, M. (2001). El cyberstalking es una extensión de la modalidad física de stalking., "Cyberstalking: Dangers on the Information Superhighway", National Center for Victims of Crime.

GÓMEZ RIVERO, Mª C.: (2011). "El derecho penal ante las conductas de acoso persecutorio", en Martínez González, Mª (dir.) El acoso: tratamiento penal y procesal, Valencia.

GOYENA HUERTA, J. (2015). De las circunstancias que agravan la responsabilidad criminal, Comentarios Prácticos al Código Penal. Tomo I (parte general. Artículos 1-137). 1ª ed.

HUBBARD, J. A. DODGE, K. A., CILLESSEN, A. H. N., COIE, J. D. Y SCHWARTZ, D. (2001). The Dyadic Nature of Social Information Processing in Boys' Reactive and Proactive Aggression. *Journal of Personality and Social Psychology*, 80.

HUBBARD, J. A., SMITHMYER, C. M., RAMSDEN, S. R., PARKER, E. H., FLANAGAN, K. D., DEARING, K. F., RELYEA, N. Et Ál. (2002). Observational, Physiological, and Self-Report Measures of Children's Anger: Relations to Reactive versus Proactive Aggression. Child Development, 73.

JIMÉNEZ SEGADO,C. (2016). La novedosa respuesta pernal frente al fenómeno sexting, Actualidad Jurídica Aranzadi núm. 917.

LARRAURI PIJOAN, E., (2009). "Igualdad y violencia de género. Comentario a la STC 59/2008", *en InDret,* Febrero

MAGRO SERVET, V.: (2015). "Los delitos de sexting (197.7) y stalking (172 ter) en la reforma del Código Penal", Ponencia de formación continuada en la Fiscalía General del Estado, 16 marzo.

MAGRO SERVET, V. (2015). Reforma del Código Penal afectante a la violencia de género, La Ley Penal, nº 114, mayo-junio.

MARTÍNEZ OTERO, J.M., (2013). La difusión de sexting sin consentimiento del protagonista: un análisis jurídico, en Derecom, núm. 12.

MELOY, J.R.: (1999). "Stalking: An old behavior, a new crime", en Psychiatric Clinics of North America, Nº22.

MELOY, J.R., & BOYD, C.: (2011). "Female stalkers and their victims", en Journal of the American Academy of Psychiatry and the Law, Nº 31,

MELOY, J.R., MOHANDIE, K., & GREEN, M.: (2013). "The Female Stalker", *en Behavioral Sciences and the Law*.

MULLEN, P., PATHE, M., & PURCELL, R.: (1999). "Study of stalkers", en American Journal Psychiatry, Nº 156.

MUÑOZ CONDE, F. Análisis de las Reformas Penales, Presente y futuro, Tirant lo Blanch, Valencia 2015.

PERAMATO MARTÍN, T. (2016). Sexo y género. Dificultades de aplicación de la nueva agravante de discriminación por razón de género, en *El Derecho Editores/Revista de Jurisprudencia nº* 2, marzo.

PUENTE ABA, L.M., (2007). Delitos contra la intimidad y las nuevas tecnologías, en *Eguzkilore,* núm. 21.

RAMÍREZ, J. M. Y ANDREU, J. M. (2003). Aggression's Typologies. International Review of Social Psychology, 16.

RAINE, A., DODGE, K., LOEBER, R., GATZKE-KOPP, L., LYNAM, D., REYNOLDS, C., STOUTHAMER-LOEBER Et Ál. (2006). The Reactive-Proactive Aggression Questionnaire: Differential Correlates of Reactive and Proactive Aggression in Adolescent Boys. *Aggressive Behavior*, 32.

REBOLLO VARGAS,R (2015).La agravante de discriminación por razón de sexo y su fundamento (art. 22.4 del Código Penal), en *Revista General de Derecho Penal* 23

SERGIO CÁMARA, A. (2016). La primera condena en España por acecho o stalking. Revista Unir junio Documento en línea. .(Ultimo acceso el 25 ,mayo 2017) http://www.unir.net/derecho/revista/noticias/la-primera-condena-en-espana-por-acecho-o-stalking/549201499291/

VÁZQUEZ-PORTOMEÑE SEIJAS, F. (2016). Violencia contra la mujer: manual de derecho penal y proceso penal: adaptado a la Ley 1/2015, de reforma del Código Penal. *Revista Aranzadi de Derecho y Proceso Penal*, núm 56.

VILLACAMPA ESTIARTE, C.: (2009). *Stalking y derecho penal. Relevancia jurídico-penal de una nueva forma de acoso*, Ed. Iustel, Madrid,.p 32.

VILLACAMPA ESTIARTE, C.: (2010). "La respuesta jurídico-penal frente al stalking en España: presente y futuro", *en ReCrim.*

CONCLUSIONES GENERALES

CONCLUSIONES GENERALES

PRIMERA. La protección de datos de carácter personal, tanto en el Ordenamiento Jurídico español como en el plano comparado, es un derecho fundamental de relativamente reciente aparición si se le compara con otros de larga tradición, como el honor o la libertad de expresión. No es de extrañar si se tiene en cuenta la relación lógica que éste mantiene con el desarrollo de la tecnología, especialmente la informática, y la necesidad de reaccionar frente a los riesgos que ésta puede representar para la libertad y la intimidad de los ciudadanos. La Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal, entronca con una rama fundamental de nuestro Derecho, como es la rama constitucional. Y esto se desprende, sin lugar a dudas, nada más comenzar a leer la misma puesto que en su artículo 1 se consagra el derecho al honor y a la intimidad personal y familiar, precepto que a todas luces entronca con el consagrado en el artículo 18 de nuestra Constitución. Estos derechos, no hacen más que consagrar dentro del marco de las libertades personales la expresión de un derecho global a la privacidad, que de una u otra manera coincide con el derecho a la intimidad entendido en sentido amplio, es decir, como derecho a la autodeterminación de la vida privada. El derecho a la privacidad comprende el reconocimiento de todos los derechos recogidos en el artículo 18 de nuestra Constitución.

SEGUNDA: El empleo de aviones no tripulados ha generado una controversia notable, dado que actualmente, diversos estados han potenciado como instrumento letal para llevar a cabo las campañas de

ataques selectivos contra miembros de grupos terroristas trasnacionales. Ante este panorama la opinión pública puede mantenerse reacia a vislumbrar las potencialidades que representa la labor de los drones y en este sentido según este artículo, la ingente labor de videovigilancia y control que podrían realizar los Drone en las infraestructuras críticas, no en vano existe una preocupación generalizada en los estados a la que no es ajena España, o Europa, por la protección de este tipo de instalaciones ante amenazas deliberadas y en particular las amenazas terroristas actuales. Creemos que con una fundamentación adecuada apoyada en un corpus legal y normativo consensuado, sería posible incluir a los drones como elemento de seguridad en las infraestructuras críticas para ejercer labores de vigilancia y control de la propia infraestructura, que redunden en la más alta protección posible ante cualquier amenaza y en particular la amenaza terrorista. Por otra parte, el uso de los Drone también ha evidenciado la necesidad de articular y armonizar normativas para la salvaguarda de los derechos de la esfera personal de los posibles ciudadanos captados. La protección de datos de carácter personal, tanto en el Ordenamiento Jurídico español como en el plano comparado, es un derecho fundamental de relativamente reciente aparición si se le compara con otros de larga tradición, como el honor o la libertad de expresión. No es de extrañar si se tiene en cuenta la relación lógica que éste mantiene con el desarrollo de la tecnología, especialmente la informática, y la necesidad de reaccionar frente a los riesgos que ésta puede representar para la libertad y la intimidad de los ciudadanos.

TERCERA: La Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal, entronca con una rama fundamental de nuestro Derecho, como es la rama constitucional. Y esto se desprende, sin lugar a dudas, nada más comenzar a leer la misma puesto que en su artículo 1 se consagra el derecho al honor y a la intimidad personal y familiar, precepto que a todas luces como decíamos, entronca con el consagrado en el artículo 18 de nuestra Constitución. Estos derechos, no hacen más que consagrar dentro del marco de las libertades personales la expresión de un derecho global a la privacidad, que de una u otra manera coincide con el derecho a la intimidad entendido en sentido amplio, es decir, como derecho a la autodeterminación de la vida privada. El derecho a la privacidad comprende el reconocimiento de todos los derechos recogidos en el artículo 18 de nuestra Constitución. El principio de información que se describe en la LOPD exige que se deberá previamente, ser informados los interesados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de su recogida y de los destinatarios de los mismos (artículo 5 LOPD). Cuestión esta que planteamos de compleja aplicación respecto al uso de drones con fines de videovigilancia por parte de las autoridades y del mismo modo la que los particulares pudieran captar, fuera del rango de acción de la contemplada como zona de su uso privado. Por este motivo es importante que la ciudadanía conozca las repercusiones que subyacen del empleo de las tecnologías drones, aplicadas a la seguridad y a la vigilancia, donde igualmente los operadores civiles de los Drone, deberán también conocer

no solo las obligaciones normativas de su uso sino también, con mayor énfasis, las consecuencias y responsabilidades derivadas de sus actividades sobre los derechos a la protección de datos y la privacidad de la ciudadanía. En este sentido, sea quien fuere el titular del Drone, la normativa le exige el cumplimiento del principio de información, debiendo ser publicado o publicitado, incluyendo la identidad del operador del dron o su representante, así como los derechos que asisten a los sujetos titulares, dado que reconoce la propia ley que si el ciudadano desconoce o no es consciente de la presencia de un Drone, este no podrá ejercer de manera adecuada los derechos que le asisten respecto al tratamiento de su imagen como dato personal, sin poder ejercer por tanto de manera concreta sus derechos ante el operador del Drone, en principio ante la legislación dispuesta a través de ARCO, y cuando entre la nueva trasposición del nuevo 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). También la LOPD describe, que este consentimiento habrá de ser expreso y por escrito si los drones se emplean en espacios que, por su naturaleza o características, pueden comportar la captación de imágenes que pudieran revelar la ideología, afiliación sindical, la religión o las creencias de las personas afectadas, en donde a tenor de esta línea de trabajo, el Grupo Europeo en Ética de las Ciencias y las Nuevas Tecnologías, observa que las empresas privadas como las autoridades públicas, deberán

adoptar los principios de las PET en el desarrollo de las nuevas tecnologías de vigilancia y seguridad, implementadas entre otros en los mecanismos Drone, entendiendo el grupo europeo en Ética de las Ciencias y la Nuevas Tecnologías que «los valores europeos de dignidad, libertad y justicia deben tenerse en cuenta antes, durante y después del proceso de diseño, desarrollo y ejecución de esas tecnologías. Las tecnologías de protección de la intimidad deben incorporarse desde la fase inicial y no añadirse como un apéndice posteriormente».

CUARTA: La carencia de una normativa concreta y explicita respecto a los usos de los Drone, y su incursión como elemento que entra en colisión con la naturaleza de distintos derechos de la esfera personal, deberá atenderse al marco legal existente en materia de protección de datos, puesto que los problemas que los drones plantean en relación con la protección de datos no son nuevos, puesto que la tecnología de la que se brinda, esto es la video imagen ya no representa ninguna novedad, pues tan solo representa una novedad y desafío al derecho, el vehículo que la porta y transporta y que basa esta novedad, en configurarse como una herramienta que dispone de una muy versátil movilidad, en un reducido tamaño, la posibilidad de resultar invisible o difícilmente detectable por el usuario de la vía pública, la posibilidad de disponer de criterios preinstalados de captación aleatoria de imágenes con fines de realizar perfiles y la accesibilidad a cualquier usuario para su adquisición.

QUINTA: Si bien en España no se le ha prestado la importancia que en otros países ha supuesto la videovigilancia tales como Reino Unido o EEUU, la

realidad en nuestro país nos muestra a través de las encuestas realizadas por el Centro de Investigaciones Sociológicas, durante los años 2008, 2009 y 2011, que en general se muestra un elevado nivel de apoyo al uso de cámaras, con cifras similares a las extraídas de encuestas de otros países citados, en donde esta se constituye generalmente como la primera medida preventiva de seguridad al incrementar la percepción de seguridad y protección ciudadana, considerándose una medida eficaz en la lucha contra la delincuencia. La contribución a la dispensa de seguridad que esta ofrece es palpable al comprobarse su utilidad como aportación de pruebas durante el proceso penal es de primer orden, en cuanto tiene eficacia probatoria para formar la convicción de un tribunal sobre la existencia de un hecho o sobre la identidad de sus autores y participes coadyuvando a la persecución del delito y como herramienta disuasoria de ilícitos penales o comportamientos incívicos.

SEXTA: La relación entre la prevención de los delitos mediante la tecnología monitorizada genera emotivos debates por una parte de la comunidad en donde se considera que esta invade parcelas de la intimidad personal, habiendo sido clara y concisa la jurisprudencia al considerar que habrá que valorar si se cumple en cada caso concreto una proporcionalidad entre los derechos afectados y el beneficio público, si bien en general puede afirmarse que existe dicha proporcionalidad, dados los límites impuestos en la utilización de la videovigilancia y las garantías (legales, procedimentales y jurisdiccionales) establecidas legalmente para los ciudadanos interpretando generalmente como válidas la toma de imágenes

de sospechosos de manera velada o subrepticia en los momentos en los que se supone fundadamente que se está cometiendo un hecho delictivo, pues ningún derecho queda vulnerado en estos casos al considerarse imágenes captadas sin estar previstas, por operar la casualidad de producirse donde se usan cámaras que filman lo que por azar ocurre delante de ellas permitiendo al órgano juzgador probar mediante el visionado de las imágenes encartadas en el proceso penal, de una manera fiable y elocuente, toda la visión del iter delictivo que pudiera escapar a los juicios de la objetividad en la declaración de cualquier sujeto incurso en la misma. Debemos por tanto considerar que respecto a su valor procesal, las grabaciones no suponen prueba distinta a que pudiera suponer una declaración que se ampara en la percepción visual.

SEPTIMA: Respecto a la adecuación legista a las nuevas tecnologías descritas, en donde la video-grabación inteligente está tomándose en consideración por las autoridades dedicando esfuerzos en investigación y desarrollo de nuevos y más eficientes métodos de video-grabación inteligente, hemos de concluir que la legislación española actual presenta dificultades para poder responder a la misma velocidad que la tecnología ofrece sus productos, y que incluso actualmente carece de reconocimiento en concreto a la que debería tener especial incidencia como la propia ley de enjuiciamiento criminal debiéndose reiterar la necesidad de exigir al poder ejecutivo y al poder legislativo que se haga efectiva una urgente regulación legislativa completa de este medio de investigación y prueba en el proceso penal que rellene la profunda laguna existente, adecuándose incluso a los

venideros sistemas de videovigilancia inteligente, con el objeto de no posibilitar vacíos legales que puedan originar inseguridad jurídica y, por consiguiente, ineficacia.

OCTAVA: La sustentación de dotar a la policía de cámaras de videograbación no cabe duda que tiene como alcance, además tratar de hacer propios los hallazgos de las investigaciones realizadas en los distintos países al objeto de constatar una mejora en las relaciones entre la policía y la comunidad, en nuestro caso, en España, cabe aducir tal finalidad como fin paralelo a la necesaria satisfacción como valor probatorio de la prueba, en este caso, la prueba videográfica, y que consiste en la captación de imágenes que determinen y configuren el iter criminis del delito, permitiendo si cabe, identificar al autor del hecho delictivo o de las personas sospechosas de realizarlo, y documentadas en soporte videográfico. Estas imágenes suponen hechos de interés para la investigación de infracciones penales, siendo también posible su utilización para asegurar la convivencia ciudadana, la erradicación de la violencia, la utilización pacífica de las vías y espacios públicos, así como la prevención de comisión de delitos, faltas e infracciones relacionadas con la seguridad pública, siendo válida por tanto la toma de imágenes de sospechosos de manera velada o subrepticia en los momentos en los que se supone fundadamente que se está cometiendo un hecho delictivo, pues ningún derecho queda vulnerado en estos casos al considerarse imágenes captadas sin estar previstas, por operar la casualidad de producirse donde se usan cámaras que filman lo que por azar ocurre delante de ellas, sobre todo, cuando acaba de empezar a ocurrir cualquier

hecho a tenor de las flagrantes imágenes, valorándose sin apreciar por ello, infracción alguna de derecho fundamental, que pudiera declarar nulo el resultado probatorio obtenido por las cámaras de uso policial en los uniformes de los agentes de policía, permitiendo al órgano juzgador probar mediante el visionado de las imágenes encartadas en el proceso penal, de una manera fiable y concisa, toda la visión del iter delictivo que pudiera escapar a los juicios de la objetividad en la declaración de cualquier sujeto incurso en la misma, pues debemos considerar que respecto a su valor procesal, la grabaciones no suponen prueba distinta a que pudiera suponer una declaración que se ampara en la percepción visual, en tanto que la jurisprudencia considera que la grabación no hace otra cosa que perpetuar la percepción que pudieran tener una o varias personas, entendiendo la jurisprudencia, que es legal la actuación basada en la imagen videográfica en los casos de investigación criminal y en los casos que exista razonable riesgo para la seguridad ciudadana o peligro concreto, conforme a derecho

NOVENA: La observancia por tanto de la legislación en España al respecto de la toma de imágenes por parte de las fuerzas y cuerpos de seguridad, demuestra el encaje legal de una posible asunción por parte de las fuerzas y cuerpos de seguridad españolas del uso de las cámaras policiales integradas en el uniforme policial, tal es el caso, de la investigación que se lleva a cabo en la policía canaria, emulando la investigación llevada a cabo en el Reino Unido en la isla de Wight. Por nuestra parte, consideramos necesaria una mayor puesta en práctica en España, llevando a cabo y desarrollando nuevas investigaciones con los diferentes cuerpos de policía

estatales. A nuestro juicio, la utilización de videograbación por parte de los agentes de policía como instrumento del desarrollo profesional de la labor policial, no presupone de partida la puesta en riesgo, de cuestiones éticas y de privacidad o pueda suponer un atentado al derecho al honor de los posibles encartados, siempre y cuando se establezca el debido protocolo ya descrito, que somete a las fuerzas y cuerpos de seguridad en el ejercicio de sus funciones, valorándose en cada caso concreto, una proporcionalidad entre los derechos afectados y el beneficio público de la obtención de las posibles imágenes de un hecho delictivo, y el sometimiento de cualquier dato obtenido mediante videograbación, a los protocolos de la ley de protección de datos vigente.

DECIMA: La falta de una base jurídica concisa en la legislación española actual, evidencia la ambigüedad legista del alcance y del límite en el uso de videograbación y de las posibilidades del uso de videocámaras por parte de la policía como herramienta del desenvolvimiento profesional, pues aunque desde el ámbito legista se entiende que la toma de imágenes resulta un medio invasivo, también entiende que resulta un medio legítimo el monitorizar escenas y acontecimientos presuntamente delictivos, desprendiéndose del enunciado del art 1.1 de la Ley, que aun considerando motivos de seguridad pública, la utilización de la video-vigilancia por las Fuerzas y Cuerpos de Seguridad, deberá respetar el principio de proporcionalidad solventando a su vez, las necesidades de idoneidad y de intervención mínima, exigiendo la existencia de un riesgo razonable para proceder a la videograbación y que en ningún caso, importante al objeto de

nuestro artículo para desprenderse de este uso aflicciones y posibilidades de revictimiacion, no podrán tomarse imágenes ni sonidos del interior de las viviendas, salvo consentimiento del titular o autorización judicial, cuando se afecte de forma directa y grave a la intimidad de las personas, respetándose escrupulosamente las normas relacionadas con el periodo de conservación de imágenes, destrucción de estas, o su revelación y puesta a disposición de las autoridades judiciales.

UNDECIMA: Respecto al tratamiento como dato de las imágenes captadas por parte de la policía, y esta a su vez estar sometida y amparada por la regulación de protección de datos, es imprescindible que se pueda realizar tratamientos con ella, esto es formar parte de un fichero que facilite su acceso, posibilitando el trasmitir o difundir estos datos videograbados, y en donde se muestre o identifique a un sujeto sobre un soporte material cualquiera, y es por esta posibilidad, que se requiere una motivación suficiente antes de posibilitar la implementación de videocámaras de uso policial en los uniformes de los profesionales de la seguridad, siendo necesario argumentar protocolos de conservación de los datos obtenidos por las fuerzas policiales, debiéndose apelar a una nueva ley que sustituya a la actual, tan obsoleta como inadaptada, dado que en su consideración, estaba destinada antaño a una salvaguarda mercantil para casos periodísticos e intereses personalísimos, obviando actualmente la citada ley, la potencialidad de las nuevas tecnologías de la imagen.

DUADÉCIMA: El uso de cámaras de videograbación continua como integración en los uniformes de policía se está expandiendo en distintos

países estando a la cabeza de estos los Estados Unidos de América. Estadísticamente según el último reporte de la principal empresa suministradora de dispositivos de videograbación portátiles , se estima que prestan sus servicios a cerca de 6.000 departamentos policiales, (aproximadamente la mitad de todos los existentes en EEUU), sumando sus efectivos más de 30.000 cámaras de videograbación continúa solo en los EEUU, a los que se acompaña desde el ámbito legislativo el desarrollo y acomodamiento de la medida en más de 35 estados mediante proyectos de ley que haga frente a la nueva realidad del ejercicio profesional y desenvolvimiento de la actuación policial del país. Esta nueva realidad obedece a distintos propósitos que se han evidenciado en diversas investigaciones que referiremos a continuación y entre los que destacamos el propio desarrollo profesional y la necesaria evidencia constatable de la actuación y ejecución por parte del agente de policía al ejecutar su trabajo, cuando esta pudiere estar en duda al necesariamente deberse en ocasiones, ejecutar mediante el uso de la fuerza. No obstante, el uso de cámaras de videograbación continua en los uniformes policiales está abierto al debate del cómo y cuándo las grabaciones pueden afectar o revictimizar a la ciudadanía por el uso inadecuado de los productos obtenidos mediante imagen. Cuestiones como la duración y permanencia de las videograbaciones en los servidores públicos, el acceso a estos, o cuestiones como el derecho al olvido, son cuestiones que circundan la viabilidad de la medida

DÉCIMO TÉRCERA: La Ley 4/1997 indica que respecto al establecimiento

de cámaras fijas en lugares públicos, se requerirá la previa autorización del Delegado del Gobierno en la Comunidad Autónoma, previo informe favorable de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la Comunidad Autónoma respectivamente, pero algo menos concreto resulta el trámite de autorización de cámaras móviles, que requieren únicamente la autorización del máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad del Estado, quien lo pondrá en conocimiento de la comisión en un plazo de setenta y dos horas según el art. 5.2, desprendiéndose en consecuencia, que está sustentada la norma , cuando se autoriza la instalación tanto de cámaras estables como móviles en espacios públicos, bajo la existencia de un riesgo razonable para la seguridad publica en el caso de las cámaras fijas y de un peligro concreto para el uso de las cámaras móviles, todo ello conforme a las ponderaciones y exigencias racionales de proporcionalidad e idoneidad y que veremos en el epígrafe dedicado al valor probatorio de la prueba videográfica.

FUENTES GENERALES

FUENTES GENERALES

ACED FÉLEZ, E., (2003). "La protección de datos personales y la videovigilancia". Revista electrónica de la Agencia de Protección de Datos de la Comunidad de Madrid, *datospersonales.org*, nº 5.

ACED FÉLEZ, E., (2013). Drones: una nueva era de la vigilancia y de la privacidad, *Seguritecnia,* núm. 403.

AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO. (2012).*Código de Comercio*. Imprenta Nacional de la Agencia Estatal.

AGUILERA LÓPEZ, P. (2014) .*Seguridad informática*. Edit. Editex. 2010, pag.

AKERMAN, B: *Antes que nos ataquen de nuevo.* La defensa de las libertades en tiempos de terrorismo, Barcelona, Península, 2007

ALEGRÍA GINER, A, C. (2011). Aproximación psicológica de la victimología. Revista de derecho y criminología, Anales de Derecho.Murcia.

ALMUZARA ALMAIDA, C.; COUDERT, F.; MARZO PORTERA, A. y NAVALPOTRO NAVALPOTRO, Y. (2007). *Estudio práctico sobre la protección de datos de carácter personal, 2ª edic*. Edit. Lex Nova.

ALONSO DE ESCAMILLA, A. (2013). El delito de Stalking como nueva forma de Acoso. Cybertalking y nuevas realidades, *La Ley Penal*, nº 105, Noviembre-Diciembre

ALONSO UREBA, A. (Dir). (2007) Código Comercio y Leyes Mercantiles. Edit. La Ley..

ALVAREZ CONDE, E y GONZALEZ, H. (2006*), Legislación terrorista comparada después de los atentados del 11 de septiembre y su incidencia en el ejercicio de los derechos fundamentales,* Real Instituto Elcano, Área Terrorismo Internacional, *ARI* n. 7

ALVAREZ ALVAREZ, L,A y PERDOMO CORDERO,C., (2015) "Inteligencia, Cibereguridad y Ciberdefensa; nuevas implicaciones conceptuales en las Estrategias de Seguridad Nacional."

ÁLVAREZ HERNANDO, J. (2011) . Guía práctica sobre Protección de

Datos: cuestiones y formularios (e-book). Edit. Lex Nova.

AMOR, P. J. (2005). Personalidades violentas. *Revista Crítica*, 925.

ANDERSON, D.E., (2010) "Drones and the Ethics of War", *Religion & Ethics NewsWeekly*, 14 May.

ANDREU, J. M. RAMÍREZ, J. M. Y RAINE, A. (2006). Un modelo dicotómico de la agresión: valoración mediante dos autoinformes (CAMA y RPQ). *Revista de Psicopatología Clínica, Legal y Forense*, 5.

ARIEL, B., (2012). Deterrence and moral persuasion effects on corporate tax compliance: findings from a randomized controlled trial. Criminology, 50.

ARIEL, B. FARRAR W, SUTHERLAND A., (2015). The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial. Revista Journal of Quantitative Criminología, Volume 31, Issue 3.

ARIAS POU, M. (2006). *Manual práctico de comercio electrónico*. Edit. La Ley.

ARZOZ SANTISTEBAN, X.,(2010).*Videovigilancia, seguridad ciudadana y derechos fundamentales*, Civitas, Madrid.

BANDURA, A. (1982). Teoría del aprendizaje social. Madrid: Espasa Calpe.

BARBER, B. R. (2009). *Internet, Derecho y Política: las transformaciones del derecho y la política en 15 artículos*. Edit. OUC.

BARRIENTOS, A, et al., (2007). Vehículos aéreos no tripulados para uso civil. Tecnología y aplicaciones. Universidad Politécnica de Madrid.

BENJAMIN, M., (2013). *Drone Warfare. Killing by Remote Control*, Brooklyn, Verso, fully revised and updated.

BLANCO NAVARRO, J, Mª Y DÍAZ MATEY, G., (2015). Presente y futuro de los estudios de inteligencia en España. Documento marco IEEE.

BUSHMAN, B. J. Y ANDERSON, C. A. (2001) Is it Time to Pull the Plug on the Hostile versus Instrumental Aggression Dichotomy? *Psychological Review*, 108.

CARRILLO RUIZ, J,A et al., (2013). "Big data en los entornos de

defensa y seguridad" documento resultado del grupo de trabajo sobre big data, de la comisión de investigación de nuevas tecnologías del centro superior de estudios de la defensa nacional. (CESEDEN) Documento de Investigación del Instituto Español de Estudios Estratégicos (IEEE)

CEREZO DOMÍNGUEZ, A.I., (2010). El protagonismo de las víctimas en la elaboración de las leyes penales, de. Tirant lo Blanch, Valencia.

CHARTRAND, T. L., & BARGH, J. A., (1999). The chameleon effect: The perception–behavior link and social interaction. Journal of personality and social psychology,76,

CLARKE, R.; ROUFFAER, C. and SÉNÉCHAUD, F., (2012) "Beyond the Call of Duty: why shouldn't video game players face the same dilemmas as real soldiers?", *International Review of the Red Cross*, Vol. 94, núm. 886.

CLARKE, R., (2014).«The regulation of civilian drones' impacts on behavioural privacy», *Computer Law and Security Review*, núm. 30.

CHAUX, E. (2003). Agresión reactiva, agresión instrumental y ciclo de la violencia. *Revista de Estudios Sociales*, 15.

Columbia law school human rights clinic and center for civilians in conflict, *The Civilian Impact of Drones: Unexamined Costs, Unanswered Questions*, New York, 2012.

CONDE ORTIZ, C. (2005). La protección de datos personales: Un derecho autónomo con base en los conceptos de intimidad y privacidad. Edit. Dykinson.

CURBET, J.: (2007). Temeraris atemorits. L'obsessió contemporània per la seguretat, Girona, CCG Edicions.

DEL PESO NAVARRO, E. (2009). *Vocabulario español actualizado de Iustecnología de la información*. Edic. Diaz de Santos, S.A.

DEL PESO NAVARRO, E.; JOVER PADRÓ, J. y DEL PESO RUIZ. M. (2004) .*Los datos de los ciudadanos en los Ayuntamientos*. Edic. Díaz de Santos, S.A.

DE LA CUESTA ARZAMENDI, J.L. y MAYORDOMO RODRIGO, V.: (2011) "Acoso y Derecho penal", *en Eguzkilore,* Nº 25.

DE LA CUESTA ARZAMENDI, J.L. (2012). Hacia una Justicia

Victimal. Encuentro Internacional en homenaje al Prof. Dr. H.c. Antonio Beristaín. *Eguzkilore Cuaderno del Instituto Vasco de Criminología* nº 26-San Sebastián,

DÍAZ, A., (2006) "La adaptación de los servicios de inteligencia al terrorismo internacional*" ARI Nº 52-*

DÍAZ LÓPEZ, J.A., (2013). El odio discriminatorio como agravante penal. Sentido y alcance del art. 22.4 CP, Civitas, Madrid.

DOVAL PAÍS, A. (2015). Nuevos límites penales para la autonomía individual y la intimidad, Thomson Reuters Aranzadi. Cizur Menor.

DZIEWECZYNSKI, T. L., EKLUND, A. C., & ROWLAND, W. J., (2006). The actor and the observer: Divergent perceptions of the causes of behavior. Morristown, NJ: General Learning Press.

ELODI VILLENA, M., (2014). «El uso de vehículos aéreos no tripulados (drones) en las labores de seguridad y vigilancia de la Administración», en *Congreso Derecho TICS - SICARM 2014*, Barcelona, 23-24 de octubre.

ECHEBURÚA, E. BACA, E. TAMARIT J, M. (2006). "Manual de Victimología". Editorial Tirant Lo Blanch. Valencia.

ECHEBURÚA, E, Y SÁEZ, M.S.C. (2015). De ser víctimas a dejar de serlo: un largo proceso. *Revista de victimología/ Journal of Victimology,*

ETXEBERRIA GURIDI, J.F., (2011). La Comisión de Videovigilancia y Libertades del País Vasco. En: Videovigilancia: ámbito de aplicación y derechos fundamentales afectados, en particular la protección de los datos personales. Valencia: Tirant lo Blanch.

FELSON, R. B. (2002). Violence and Gender. Reexamined. Washington D. C.: *American Psychological Association.*

FINN, R.L., WRIGHT, D., (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. ELSEVIER.

FOUCAULT, M., (1995). Discipline & punish: The birth of the prison. Vintage.

GARCÍA GONZÁLEZ, J.: (2010). Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, Tirant lo Blanch,

Valencia.

GARCÍA MERCADER, E, J. Y GARCÍA GARCÍA, C. (2015). Victimología y víctima de violencia de género; Hacia una atención integral. coord. Nicolás Guardiola, Juan J., Giner Alegría, Cesar Augusto, Nicolás García, José Neftalí. Iuris Universal Ediciones.

GARAIGORDOBIL, M. Y OÑEDERRA, J. A. (2010), La violencia entre iguales. Revisión teórica y estrategias de intervención. Madrid: Pirámide.

GARRIDO GENOVÉS, V.: (2001). Amores que matan. Acoso y violencia contra las mujeres. Alzira, Algar.

GARRIDO ROBRES, J, A., (2006). *¿Sería conveniente una especialidad fundamental de inteligencia para las Fuerzas Armadas Españolas? Estudio de esta especialidad en otras Fuerzas Armadas*. Madrid, ESFAS,

GERVAIS, W. M., & NORENZAYAN, A., (2012). Like a camera in the sky? Thinking about God increases public self-awareness and socially desirable responding. Journal of Experimental Social Psychology, 48.

GREGORIE, M. (2001). El cyberstalking es una extensión de la modalidad física de stalking., "Cyberstalking: Dangers on the Information Superhighway", National Center for Victims of Crime.

GUERRERO LEBRÓN, M. J., (2014). «La regulación transitoria de los operadores de aeronaves civiles pilotadas por control remoto», *La Ley mercantil,* Editorial La Ley. 31 de julio.

GUERRERO LEBRÓN, M. J., CUERNO REJADO, C., MÁRQUEZ LOBILLO, P., (2013) "Aeronaves no tripuladas: Estado de la legislación para realizar su integración en el espacio aéreo no segregado", *Revista de Derecho del Transporte,* Nº. 12.

GÓMEZ RIVERO, Mª C.: (2011). "El derecho penal ante las conductas de acoso persecutorio", en Martínez González, Mª (dir.) El acoso: tratamiento penal y procesal, Valencia.

GOÑI SEIN, J. L. (2007). .*La videovigilancia empresarial y la protección de datos personales*. Edit. Thomson Civitas.

GOYENA HUERTA, J. (2015). "De las circunstancias que agravan la responsabilidad criminal". Comentarios Prácticos al Código Penal. Tomo I

(parte general. Artículos 1-137). 1ª ed.

GUDIN, F. (2006), *La lucha contra el terrorismo en la sociedad de la información,* Madrid: Edisofer.

HALLA, A.R., COYNEA, C.J., (2013).The political economy of drones. Routledge - Taylor & Francis Group.

HEYNS, C., (2013). *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Doc. ONU A/68/382, 13 de septiembre.

HUBBARD, J. A. DODGE, K. A., CILLESSEN, A. H. N., COIE, J. D. Y SCHWARTZ, D. (2001). "The Dyadic Nature of Social Information Processing in Boys' Reactive and Proactive Aggression". *Journal of Personality and Social Psychology, 80.*

HUBBARD, J. A., SMITHMYER, C. M., RAMSDEN, S. R., PARKER, E. H., FLANAGAN, K. D., DEARING, K. F., RELYEA, N. Et Ál. (2002). Observational, Physiological, and Self-Report Measures of Children's Anger: Relations to Reactive versus Proactive Aggression. Child Development, 73.

IRAVEDRA, J. C.: (2011) «Inteligencia de fuentes abiertas en la Unión Europea (proyecto Virtuoso)», Jornadas de Estudios de Seguridad, 17, 18 y 19 mayo.

JIMÉNEZ SEGADO, C. (2016). "La novedosa respuesta pernal frente al fenómeno sexting". *Actualidad Jurídica Aranzadi núm*. 917.

LARRAURI PIJOAN, E., (2009). "Igualdad y violencia de género. Comentario a la STC 59/2008", en InDret, Febrero.

LESMES SERRANO, C. (2008). *La ley de protección de datos. Análisis de su jurisprudencia*. Edit. Lex Nova..

LEWIS, M.W., (2012). "Drones and the Boundaries of the Battlefield", *Texas International Law Journal*, Vol. 47, Issue 2,

LIND, W, S.: (2004). Internet World Stats: Usage and Population Statistics. Antiwar.

MAGRO SERVET, V.: (2015). "Los delitos de sexting (197.7) y stalking (172 ter) en la reforma del Código Penal", Ponencia de formación continuada en la Fiscalía General del Estado, 16 marzo.

MAGRO SERVET, V. (2015). "Reforma del Código Penal afectante a la violencia de género", *La Ley Penal*, nº 114, mayo-junio.

RODRÍGUEZ MANZANERA, L. (2012). Derecho victimal y victimodogmática. *Eguzkilore: Cuaderno del Instituto Vasco de Victimología.*

MARTÍNEZ OTERO, J.M., (2013). "La difusión de sexting sin consentimiento del protagonista: un análisis jurídico", *en Derecom*, núm. 12.

MARTÍNEZ MARTÍNEZ, R., (2005): Una aproximación crítica a la autodeterminación informativa, Madrid, Civitas.

MARTÍN DE SANTOS, I. Y VEGA, A. M.: (2010). "Las fuentes abiertas de información: un sistema de competencia perfecta", *en Inteligencia y Seguridad: revista de análisis y prospectiva*, número 8.

MARTÍNEZ, GILBERTO L.: (2011). "Minería de datos: Cómo hallar una aguja en un pajar", Ingenierías, 53.

MATTELART, A Y VITALIS.A., (2015). De Orwell al cibercontrol. Gedisa.

McCLOSKEY, M., (2009). "The War Room: Daily Transition between Battle, Home Takes aToll on Drone Operators", *Stars and Stripes*, 27 October.

MELOY, J.R.: (1999). "Stalking: An old behavior, a new crime", en *Psychiatric Clinics of North America,* Nº22.

MELOY, J.R., MOHANDIE, K., & GREEN, M.: (2013). "The Female Stalker", *en Behavioral Sciences and the Law*

Memoria Anual 2010 de la Agencia Española de Protección de Datos. Vid: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2010/common/AEPD_Memoria_2010.pdf

Memoria Anual 2011 de la Agencia Española de Protección de Datos. Vid: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf

MELZER, N., (2013) .*Implications of the Usage of Drones and Unmanned Robots in Warfare*, Directorate-General for External Policies of the Union, European Union, Brussels, May.

MULLEN, P., PATHE, M., & PURCELL, R.: (1999). "Study of stalkers", en *American Journal Psychiatry*, Nº 156.

MUÑOZ CONDE, F. Análisis de las Reformas Penales, Presente y futuro, Tirant lo Blanch, Valencia 2015.

NAVARRO, D. (2012). *La UE crea el 'derecho al olvido' en la red*". 26.01.Diario La Vanguardia

NAVARRO, D. (2004). El ciclo de inteligencia y sus límites. *Cuadernos Constitucionales de la Catedra Fadrique Furió Ceriol, Vol. 48*.

NICOLÁS GUARDIOLA, J, J, GARCÍA MERCADER, E, J, GINER ALEGRÍA, C, A. (2013). Ciencias Jurídicas y Victimológicas; Derechos Humanos en el contexto de la Victimología y la marginación. Thomson Reuters Aranzadi.

PARDO, M.; RUBIO, E.; GÓMEZ, F. y ALFONSO, R. "La protección de los datos de carácter personal como Derecho Fundamental autónomo". Universidad de Murcia

PAUNER CHULVI, C., (2016) "El uso emergente de drones civiles en España. Estatuto jurídico e impacto en el derecho a la protección de datos" *Revista de Derecho Político* UNED, N.º 95, enero-abril

PIÑAR MATAS, J. L. y CANALES GIL, Á. (2011) . *Legislación de protección de datos*, Portal Derecho, S.A.,

PÉREZ FRANCESCH, J.L. /GIL MARQUEZ, T; (2015) .El terrorismo global, UOC, Barcelona.

PEGUERA POCH, M. (2005). Derecho *y nuevas tecnologías*. Edit. OUC.

PEW RESEARCH CENTER, (2013). "Report questions drone use, widely unpopular globally, but not in the U.S", Washington, D.C., October 23,

PERAMATO MARTÍN, T. (2016). Sexo y género. Dificultades de aplicación de la nueva agravante de discriminación por razón de género, en *El Derecho Editores/Revista de Jurisprudencia nº* 2, marzo.

PUENTE ESCOBAR, A. (2008). "Reflexiones sobre el desarrollo reglamentario de la ley Orgánica de Protección de Datos". *Protección de Datos II. Boletín colegio de abogados de Madrid. Núm.5. Madrid.*

PUENTE ABA, L.M., (2007). "Delitos contra la intimidad y las nuevas tecnologías", en *Eguzkilore,* núm. 21.

RAMÍREZ, J. M. Y ANDREU, J. M. (2003). "Aggression's Typologies. International" *Review of Social Psychology*, 16.

RAINE, A., DODGE, K., LOEBER, R., GATZKE-KOPP, L., LYNAM, D., REYNOLDS, C., STOUTHAMER-LOEBER Et Ál. (2006). The Reactive-Proactive Aggression Questionnaire: Differential Correlates of Reactive and Proactive Aggression in Adolescent Boys. *Aggressive Behavior,* 32.

RAWLS, J (1996): Sobre las libertades, Barcelona, Paidós.

REBOLLO PUIG, M.; IZQUIERDO CARRACO, M.; ALARCÓN SOTOMAYOR, L. y BUENO ARMIJO, A. M. (2010) .*Derecho administrativo sancionador*. Edit. Lex Nova.

REBOLLO VARGAS,R (2015).La agravante de discriminación por razón de sexo y su fundamento (art. 22.4 del Código Penal), en *Revista General de Derecho Penal* 23

Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston, Addendum, Study on Targeted Killings, (2016) U.N. Doc. A/HRC/14/24/Add.6.

REVENGA SÁNCHEZ, M (2007) (Director), Terrorismo y Derecho bajo la estela del 11 de septiembre, Valencia, Tirant lo Blanch.

REVENGA SANCHEZ, M. (2006*), Garantizando la libertad y la seguridad de los ciudadanos en Europa: Nobles sueños y pesadillas en la lucha contra el terrorismo*, Parlamento y Constitución, n. 20.

RODRIGUEZ CANOSA, G,R; BARRIENTOS CRUZ, A; CERRO GINER, J., (2011) .Caracterización de las infraestructuras críticas de exteriores y su influencia sobre sistemas de vigilancia robóticos.

RODRÍGUEZ LÓPEZ DE LEMUS, P. (2009). *Manual de Implantación LOPD Para Procuradores*. Edit. DNTecnologias.

RUIZ MIGUEL, C (2003): «El derecho a la protección de los datos personales en la Carta de derechos fundamentales de la Unión Europea», Revista de Derecho Comunitario, n.º 14, pp. 7-43

SERGIO CÁMARA, A. (2016). La primera condena en España por

acecho o stalking. Revista Unir junio Documento en línea. (Ultimo acceso el 25 ,mayo 2017) http://www.unir.net/derecho/revista/noticias/la-primera-condena-en-espana-por-acecho-o-stalking/549201499291/

SERRA CRISTÓBAL, R., (2015) "La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional". En *Revista de Derecho Político* N.º 92, enero-abril.

SILVA SANCHEZ, J M., (2001). La expansión del Derecho penal. Aspectos de la política-criminal de las sociedades postindustriales, 2ª ed., Madrid.

SMITH, G. J. D., (2004). Behind the screens: Examining constructions of deviance and informal practices among cctv control room operators in the uk. Surveillance and Society, 2.

STERIO, M., (2012). "The United States' Use of Drones in the War on Terror: The (Il)legality of Targeted Killings Under International Law", *Case Western Reserve Journal of International Law*, Vol. 45,

SULLIVAN, J.M., (2006). Evolution or revolution? rise of uavs. IEEE Technology and Society Magazine 25(3)

ÚBEDA DE LOS COBOS, J., (2008)."Videograbación y videoconferencia". Cuadernos de Derecho Judicial CGPJ Madrid.

UMPHRESS,D,A.: (2006). "Naufragando en el contenedor digital: el impacto que tiene la Internet en la recopilación de inteligencia de fuentes abiertas (OSINT)", *Air and Space Power Journal.*

UNITED STATES DEPARTMENT OF DEFENCE: U.S. *unmanned systems integrated roadmap (fiscal years 2009-2034)*, Washington DC, 2009.

VALERA, M. y VELASTIN, S.A., (2005). "Intelligent distributed surveillance systems: a review. Vision, Image and Signal Processing",*IEEE Proceedings,* 152.

VÁZQUEZ-PORTOMEÑE SEIJAS, F. (2016). "Violencia contra la mujer: manual de derecho penal y proceso penal: adaptado a la Ley 1/2015, de reforma del Código Penal". *Revista Aranzadi de Derecho y Proceso Penal*, núm 56.

VERGOTTINI, D (2004), *Guerra e costituzione. Nuovi conflictti e sfide alla*

democrazia, Bologna:Il Mulino.

VERVALE J (2006), *La legislación antiterrorista en Estados Unidos, ¿Inter arma silent leges?*, Buenos Aires: Ediciones del Puerto.

VILLACAMPA ESTIARTE, C.: (2009). *Stalking y derecho penal. Relevancia jurídico-penal de una nueva forma de acoso,* Ed. Iustel, Madrid.

VILLACAMPA ESTIARTE, C.: (2010). "La respuesta jurídico-penal frente al stalking en España: presente y futuro", *en ReCrim.*

VOLOVELSKY, U., (2014) «Civilian uses of unmanned aerial vehicles and the threat to the right to privacy. An Israeli case study», *Computer Law & Security Review*, núm. 30,

WALTER, M. (2006), *Terrorismo y guerra justa*, Barcelona:Centre de Cultura Contemporanea de Barcelona.

WATTS, A.C., AMBROSIA, V.G., HINKLEY, E.A., (2012). Unmanned aircraft systems in remote sensing and scienti_c research: Classi_cation and considerations of use. Remote Sensing

WHITAKER, R. (1999) *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Barcelona: Paidós.

ZABIA DE LA MATA, J. (2008) .*Protección de datos: comentarios al Reglamento*. Edit. Lex Nova.

.

OTRAS FUENTES

OTRAS FUENTES

AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO. *Código de Comercio*. Imprenta Nacional de la Agencia Estatal. 2012, pag. 61.

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y Social Europeo y al Comité de las Regiones de 25 de Enero de 2012. "*La protección de la privacidad en un mundo interconectado. Un Marco Europeo de Protección de Datos para el siglo XXI"*, COM (2012) 9 final. Texto pertinente a efectos del EEE. Vid:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PDF

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y Social Europeo y al Comité de las Regiones de 25 de Enero de 2012. "*La protección de la privacidad en un mundo interconectado. Un Marco Europeo de Protección de Datos para el siglo XXI"*. op. cit., p. 4-7

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento automatizado de sus datos personales y a la libre circulación de estos (DO L281, 23/11/95).

INNOVACION Y CUALIFICACION, S.L. *Ley Orgánica de Protección de Datos de Carácter Personal*. Edit. INNOVA. 2006, pag. 104.

Memoria Anual 2010 de la Agencia Española de Protección de Datos. Vid: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2010/common/AEPD_Memoria_2010.pdf

Orden PRE/1366/2010, de 20 de mayo, por la que se modifica el Reglamento de la Circulación Aérea Operativa, aprobado por el Real Decreto 1489/1994, de 1 de julio.

Documento 10019 o Manual sobre RPAS 2015, como una guía para los Estados y los operadores a la hora de armonizar las regulaciones con el fin de la integración de los RPAS en un espacio aéreo único y no segregado. www.wyvernltd.com/wp-content/uploads/2015/05/ICAO-10019-RPAS.pdf

COMMUNICATION FROM THE COMMISSION TO THE

EUROPEAN PARLIAMENT AND THE COUNCIL COM/2014/0207 final A new era for aviation Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0207

RIGA DECLARATION ON REMOTELY PILOTED AIRCRAFT (drones) "FRAMING THE FUTURE OF AVIATION" Riga,6 March 2015 http://www.aerpas.es/wp-content/uploads/2015/03/EU_Riga-Declaration_150306.pdf?531a11

Sentencia: Tribunal de Grande Instance de Montpellier Ordonnnance de rèfèrè Du 28/10/2010.

ICAO Cir 328, Unmanned Aircraft Systems (UAS) Order Number: CIR328
http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston, Addendum, Study on Targeted Killings, U.N. Doc. A/HRC/14/24/Add.6, par. 27 p. 9.

artículo 8.2.b del Estatuto de Roma sobre la Corte Penal Internacional. http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95.

Juan José Delgado Morán . Ucam, julio 2.018.