UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

Departamento de Derecho Administrativo

TECNOLOGÍAS DE DETECCIÓN DE PERSONAS EN LA UNIÓN EUROPEA: LA SEGURIDAD DE LOS ESTADOS DE LA UNIÓN FRENTE A LA VULNERACIÓN DE LOS DDFF DE LOS CIUDADANOS.

TRABAJO DE FIN DE MÁSTER DE ACCESO A LA ABOGACÍA

CLARA GONZÁLEZ PUENTE

Tutelado por:
D. Fernando González Botija
Profesor titular de Derecho Administrativo y Secretario Académico del Departamento de Derecho Administrativo

RESUMEN

Las nuevas tecnologías se han impuesto, en los últimos años, en el ámbito de la seguridad nacional, la vigilancia de fronteras y la investigación de delitos y persecución del crimen organizado en todo el mundo. La proliferación de este tipo de medidas de investigación tecnológica asegura una mayor efectividad de las actuaciones llevadas a cabo por los gobiernos nacionales y los cuerpos de seguridad de los estados, sin embargo, también son altamente intrusivas en la esfera de los derechos fundamentales de los ciudadanos.

Los gobiernos y las organizaciones supranacionales están intentando ponerse al día en la regulación de estas medidas de vigilancia, pero su proliferación y la velocidad a la que se desarrollan y se propagan ha derivado en una importante insuficiencia normativa. La falta de leyes de cobertura deja la puerta abierta a la comisión de atropellos contra los derechos fundamentales de millones de personas en todo el mundo.

La proliferación del crimen organizado y del terrorismo han legitimado a los estados a la hora de tomar medidas tecnológicas de control y vigilancia muy intrusivas en la intimidad y la privacidad de los ciudadanos.

La intención de este trabajo es realizar un breve análisis de las distintas tecnologías de detección y control de personas, de la normativa que les da cobertura y de los derechos fundamentales en juego cuando estas se aplican. Para ello me serviré expresamente de la doctrina sentada en los pronunciamientos del Tribunal de Justicia de la Unión Europea, el Tribunal Europeo de Derechos Humanos y los altos tribunales nacionales.

PALABRAS CLAVE Y ABREVIATURAS

Tribunal Europeo de Derechos Humanos (TEDH), Consejo de Europa, Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH), Unión Europea (UE), Tribunal de Justicia de la Unión Europea (TJUE), Tratado de Funcionamiento de la Unión Europea (TFUE), Tratado de la Unión Europea (TUE), Derechos Humanos (DDHH), Derechos Fundamentales (DDFF), Carta de los Derechos Fundamentales de la Unión Europea, Estados Miembros (EEMM)…

SUMMARY

The use of new technologies has gained the upper hand in the course of recent years, particularly in the field of national security, border control and fight against terrorism and organized crime. The proliferation of these detection and surveillance technologies implies greater effectiveness and efficiency in the actions of security agencies and law enforcement authorities, however the downside is how highly intrusive these measures can be in the sphere of fundamental and human rights.

Governments and supranational organizations are trying to catch up with the regulation of these surveillance measures; nevertheless, their development speed has resulted in a major insufficiency of legislation that leaves the door open for the commission of offences against the rights of millions of people. The rise of terrorism and organized crime has legitimized the imposition of intrusive measures by governments, many of which interfere with the individual's intimacy and privacy.

In this context, this Project aims to identify the different detection and surveillance techniques used in the international scene. It also pursues the objective of analysing the scarce regulation that covers both the implementation of these surveillance measures and the restrictions to the exercise of rights. To address these issues, I will build along the lines of the recent rulings by the European Court of Human Rights, the Court of Justice of the European Union and national high courts.

KEY WORDS AND ABBREVIATIONS

European Court of Human Rights (ECHR), Council of Europe, European Convention on Human Rights (ECHR), European Union (EU), European Court of Justice (CJUE), Treaty on the Functioning of the European Union (TFEU), Treaty on European Union (TEU), Human Rights, Fundamental Rights, Charter of Fundamental Rights of the European Union, Member States…

ÍNDICE DE CONTENIDOS

ÍNDICE DE CONTENIDOS

I. INTRODUCCIÓN 1

II. DERECHOS FUNDAMENTALES EN JUEGO 3

1. Derecho a la vida privada 7

2. El derecho a la Protección de datos de carácter personal 10

III. TECNOLOGÍAS DE VIGILANCIA Y DE DETECCIÓN DE PERSONAS Y LA AFECCIÓN DE LOS DDFF 12

1. Circuitos cerrados de televisión y fotografía digital 14

A) Descubierto 14

B) Encubierto 23

2. Control de dispositivos de audio 24

3. Inspección del equipaje con Rayos X 28

4. Instrumentos de análisis de datos 30

5. Uso de drones 34

IV. CONCLUSIÓN. LOS SERVICIOS DE INTELIGENCIA DE LOS ESTADOS MIEMBROS DE LA UE Y LAS GARANTÍAS DE RESPETO A LOS DERECHOS FUNDAMENTALES 40

BIBLIOGRAFÍA 44

TECNOLOGÍAS DE DETECCIÓN DE PERSONAS EN LA UNIÓN EUROPEA: LA SEGURIDAD DE LOS ESTADOS DE LA UNIÓN FRENTE A LA VULNERACIÓN DE LOS DDFF DE LOS CIUDADANOS.

I. INTRODUCCIÓN

La defensa de los Derechos Fundamentales es uno de los objetivos principales de los Estados modernos en la actualidad. Tras los graves conflictos bélicos vividos en el siglo XX - y muy especialmente tras la Segunda Guerra Mundial - la conquista de estos derechos y el respeto a los mismos se convirtió en una prioridad. Estos derechos que hoy consideramos tan representativos de los países desarrollados, siguen sin estar presentes en muchos estados en vías de desarrollo, que buscan precisamente poder garantizar a sus ciudadanos su pleno ejercicio y respeto.

Las Comunidades Europeas, desde su origen, se comprometieron a exigir a los Estados Miembros el respeto a los derechos y libertades enunciados en la Declaración Universal de 1948[1]. Actualmente, la Unión Europea (en adelante, UE) continúa esforzándose día a día para que ninguna norma ni disposición de gobierno de los Estados Miembros infrinja los derechos de los ciudadanos europeos. La Carta de los Derechos Fundamentales de la Unión Europea, las Constituciones nacionales de los Estados Miembros y el Convenio Europeo de los Derechos Humanos (o CEDH) del Consejo de Europa son las principales herramientas de protección de los derechos fundamentales en la UE y son el Tribunal de Justicia de la UE y el Tribunal Europeo de Derechos Humanos los órganos encargados de controlar el cumplimiento de estos catálogos de derechos.

Sin embargo, la situación internacional en la que nos encontramos - la proliferación del terrorismo, el aumento de la cultura del odio y la aparición de grupos de extremismo político etc. - ha convertido estos instrumentos de consenso en papel mojado. Sin la intervención de los gobiernos de los Estados Miembros, el respeto a los derechos y libertades no está garantizado. Esta situación de tensión en el plano internacional, pero

[1] ***Declaración Universal de los Derechos Humanos***, Asamblea General de las Naciones Unidas. París, 10 de diciembre de 1948

también a nivel interno en muchos países del mundo, ha derivado en la necesidad de aumentar las medidas de vigilancia y control fronterizo, para garantizar la seguridad de sus ciudadanos.

Encontrar una posición de equilibrio entre estos dos conceptos tan distintos, seguridad y respeto a los derechos fundamentales, no es una tarea sencilla. Mientras los gobiernos nacionales centran sus esfuerzos en mantener la estabilidad y prevenir futuros ataques terroristas, la protección de la independencia, la libertad y la privacidad de los ciudadanos pasa a un segundo plano. De otro lado entran en juego los avances tecnológicos actuales que permiten a los cuerpos y fuerzas de seguridad de los Estados monitorizar, seguir y controlar a cualquier sujeto en cualquier lugar. Estos instrumentos innovadores, en manos de los gobiernos, pueden derivar en un abuso de sus prerrogativas que suponga la violación de los derechos fundamentales que tanto ha costado conseguir.

Los sistemas de vigilancia contemporáneos - capaces de injerir en los aspectos más privados de la vida de una persona - desarrollados a partir de esos avances tecnológicos pueden contraponerse a los principios democráticos y a los derechos y libertades conseguidos tras siglos de guerras y abusos por parte de los gobernantes. Esta intrusión no es una cuestión secundaria.

Con este trabajo se pretende, por una parte, exponer de forma breve cuáles son los derechos que se ven principalmente afectados por los sistemas de vigilancia y seguridad nacional contemporáneos. Por otra, realizar un análisis de las tecnologías más comúnmente utilizadas en el ámbito de seguridad nacional, haciendo referencia a las normas que sustentan su aplicación en el ámbito del Derecho de la Unión Europea y del Derecho Español. Para ello he contado con el apoyo de numerosas fuentes, entre ellas, la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos, que creo otorgará al lector una visión más concreta de cómo los jueces salvaguardan el respeto a los derechos fundamentales.

Las investigaciones realizadas nos harán percatarnos de la difícil tarea a la que se enfrentan legisladores, jueces y gobernantes - que persiguen el fortalecimiento de las medidas de seguridad al tiempo que el cumplimiento de los derechos fundamentales - y nos haremos una ligera idea de lo que la tecnología es capaz de abarcar en la sociedad actual.

II. DERECHOS FUNDAMENTALES EN JUEGO

El uso de las tecnologías de detección y control de personas debe entenderse en el marco de la investigación policial o el mantenimiento de la seguridad nacional. Es decir, que el uso de este tipo de mecanismos de vigilancia debe estar limitado a los casos de excepcional importancia para el mantenimiento de la seguridad o la prevención y la lucha contra el crimen organizado y el terrorismo.

La barrera de los derechos fundamentales de la persona solamente puede verse alterada por razones de interés general y por prescripción específica de la ley. En nuestro ordenamiento es la Ley Orgánica el instrumento dotado de garantía constitucional que hace posible la intervención del Estado en la esfera de los derechos de la persona.

Como sabemos, en un Estado de derecho como España o cualquiera de los veintiocho estados miembro de la Unión Europea, las leyes son creadas por el Parlamento, dentro del marco de la Constitución nacional existente y siempre respetando los instrumentos internacionales de reconocimiento y protección de los Derechos Fundamentales de las que cada estado sea parte[2]. Sin embargo, en ocasiones, el legislador se encuentra con la difícil tarea de regular nuevas realidades que pueden interferir en la protección de los derechos de la persona y que, a pesar de ello exigen una base legal que justifique y de valor a las actuaciones llevadas a cabo por el Estado. Es este punto el que nos interesa abordar ahora; ¿en qué casos puede justificarse la limitación del ejercicio y el disfrute de un derecho fundamental? ¿Cuándo está justificado éticamente y hasta qué punto?

La restricción de los derechos fundamentales en el ámbito del proceso judicial o en la prevención e investigación de delitos de todo tipo está a la orden del día; *"El concepto de «restricción de los Derechos Fundamentales» presenta una extraordinaria utilidad para el campo del Derecho. Esta circunstancia se pone de relieve a la hora de precisar las exigencias constitucionales que han de cumplir aquellos actos procesales que inciden sobre derechos fundamentales para alcanzar la eficacia procesal que*

[2] ***Constitución Española de 1978***; *Artículo 10***.** 1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social. 2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

persiguen. Es el caso, por ejemplo, de la entrada y registro domiciliario, la intervención de las comunicaciones telefónicas o las novedosas medidas relativas a la intervención y acceso de los datos de tráfico de las comunicaciones electrónicas, así como a la obtención y tratamiento del ADN e, incluso, de las medidas que cabe adoptar para luchar contra la criminalidad organizada, como la infiltración de un agente encubierto o la instalación de aparatos de escucha sobre un domicilio, cuya adopción, todos ellos, por parte del órgano jurisdiccional competente, está orientada a la consecución de los fines propios del proceso penal, civil, así como del procedimiento administrativo. Por el hecho de incidir sobre derechos fundamentales, dichas actuaciones procesales deberían constituir restricciones o limitaciones de tales derechos, lo que significa que su eficacia procesal ha de estar sometida al más estricto cumplimiento de las exigencias constitucionales que dicha calificación conlleva."[3]

Pues bien, este concepto de restricción o limitación de los Derechos Fundamentales encuentra, en el Derecho Comunitario, su fundamento en el Art. 52 de la Carta de los Derechos Fundamentales de la Unión Europea[4]; *"El alcance e interpretación de los*

[3] MARÍA JOSÉ CABEZUDO BAJO, ***"La restricción de los derechos fundamentales: un concepto en evolución y su fundamento constitucional"*** *Revista de Derecho Político de la UNED,* N.º 77, enero-abril 2010, págs. 143-182

[4] ***Carta de los Derechos Fundamentales de la Unión Europea*** (2000/C 364/01), Niza 7 de diciembre de 2000: "*Artículo 52:* 1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. 2. Los derechos reconocidos por la presente Carta que se mencionan en otras Partes de la Constitución se ejercerán en las condiciones y dentro de los límites definidos por ellas. 3. En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa. 4. En la medida en que la presente Carta reconozca derechos fundamentales resultantes de las tradiciones constitucionales comunes a los Estados miembros, dichos derechos se interpretarán en armonía con las citadas tradiciones.
5. Las disposiciones de la presente Carta que contengan principios podrán aplicarse mediante actos legislativos y ejecutivos adoptados por las instituciones, órganos y organismos de la Unión, y por actos de los Estados miembros cuando apliquen el Derecho de la Unión, en el ejercicio de sus competencias respectivas. Sólo podrán alegarse ante un órgano jurisdiccional en lo que se refiere a la interpretación y control de la legalidad de dichos actos. 6. Se tendrán plenamente en cuenta las legislaciones y prácticas nacionales según lo especificado en la presente Carta. 7. Las explicaciones elaboradas para guiar en la interpretación de la Carta de los Derechos Fundamentales serán tenidas debidamente en cuenta por los órganos jurisdiccionales de la Unión y de los Estados miembros."

Derechos y Principios". Este artículo establece en sus apartados primero y segundo los límites que pueden imponerse a los derechos enunciados en el texto. Lo hace, siguiendo la línea establecida por el TJUE en el asunto *Kjell Karlsson and Others (Cuestión prejudicial planteada por Suecia*[5]*)*, en el que se recogía el siguiente razonamiento; *"(...) según jurisprudencia consolidada, pueden establecerse restricciones al ejercicio de los derechos, en particular en el ámbito de una organización común de mercado, siempre que dichas restricciones respondan efectivamente a objetivos de interés general perseguidos por la Comunidad y no constituyan, teniendo en cuenta el objetivo perseguido, una intervención desmesurada e intolerable que afecte a la esencia misma de dichos derechos"*. El legislador europeo aclara que, cuando se refiere a "interés general" en realidad está hablando de algunos de los principios fundamentales enunciados en los Tratados fundacionales; como los enunciados en el Artículo 3 del Tratado de la Unión Europea[6], en el que se invocan los valores fundamentales de la Unión; tales como la paz, la libertad, la seguridad y la justicia, la unión de los pueblos y el respeto a su identidad nacional, o la cohesión económica y social. Son estos principios los que el legislador pretende proteger frente a todo, incluso si para ello es

[5] Sentencia del Tribunal de Justicia de 13 de abril de 2000, ***Kjell Karlsson y otros. Petición de decisión prejudicial: Regeringsrätten – Suecia,*** **C-292/97**

[6] ***Tratado de la Unión Europea*** (2016/C 202/01). *"Artículo 3 (Anterior Artículo 2*): 1. La Unión tiene como finalidad promover la paz, sus valores y el bienestar de sus pueblos. 2. La Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia. 3. La Unión establecerá un mercado interior. Obrará en pro del desarrollo sostenible de Europa basado en un crecimiento económico equilibrado y en la estabilidad de los precios, en una economía social de mercado altamente competitiva, tendente al pleno empleo y al progreso social, y en un nivel elevado de protección y mejora de la calidad del medio ambiente. Asimismo, promoverá el progreso científico y técnico. La Unión combatirá la exclusión social y la discriminación y fomentará la justicia y la protección sociales, la igualdad entre mujeres y hombres, la solidaridad entre las generaciones y la protección de los derechos del niño. La Unión fomentará la cohesión económica, social y territorial y la solidaridad entre los Estados miembros. La Unión respetará la riqueza de su diversidad cultural y lingüística y velará por la conservación y el desarrollo del patrimonio cultural europeo. 4. La Unión establecerá una unión económica y monetaria cuya moneda es el euro.

5. En sus relaciones con el resto del mundo, la Unión afirmará y promoverá sus valores e intereses y contribuirá a la protección de sus ciudadanos. Contribuirá a la paz, la seguridad, el desarrollo sostenible del planeta, la solidaridad y el respeto mutuo entre los pueblos, el comercio libre y justo, la erradicación de la pobreza y la protección de los derechos humanos, especialmente los derechos del niño, así como al estricto respeto y al desarrollo del Derecho internacional, en particular el respeto de los principios de la Carta de las Naciones Unidas. 6. La Unión perseguirá sus objetivos por los medios apropiados, de acuerdo con las competencias que se le atribuyen en los Tratados."

necesario el menoscabo de los derechos individuales, siempre que se limiten proporcional y justificadamente.

En el apartado tercero se refiere el legislador europeo al Convenio Europeo de los Derechos Humanos, instrumento inspirador de la Carta, que debe ser contemplado en el Derecho de la Unión, ya que los veintiocho miembros de la UE son estados contratantes del Convenio. La Carta establece los límites y el alcance de los derechos fundamentales conforme a lo establecido en el CEDH. El legislador europeo no duda en recordar la necesidad de respetar cualquiera de los dos textos cuando se pretenda acotar el ejercicio de los derechos fundamentales, insistiendo en que esto no implica ni la confusión de ordenamientos ni una restricción de la independencia del Derecho Comunitario. Es más, busca alejarse de la sombra proyectada por el Convenio yendo un poco más allá y estableciendo el sistema de mínimos que impide a la UE y a sus estados fijar los términos de garantía de derechos "por debajo" de las prerrogativas recogidas en el CEDH, permitiendo, sin embargo, una protección más extensa.

Finalmente, se refiere el Art. 52 a las declaraciones de derechos nacionales, presentes en las constituciones de los estados miembros, que también forman parte del sistema europeo de Derechos Fundamentales y que legitiman a los Estados a fijar sus propios límites, siempre de acuerdo a los principios de proporcionalidad e interés general referido en los párrafos anteriores.

En Derecho Español, la limitación de los derechos fundamentales se enuncia en el Artículo 55.2 de la Constitución de 1978; *"Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las leyes."* y ha sido desarrollado posteriormente por la jurisprudencia del Tribunal Constitucional y la doctrina, que insisten en defender la tesis de la limitación de derechos fundamentales basada en la proporcionalidad y el interés general.

Es importante, sin embargo, subrayar que, aunque la traba de derechos fundamentales pueda estar permitida, siempre ha de hacerse una interpretación restrictiva de los límites, tratando de favorecer la eficacia y esencia de los derechos afectados. Este es el principio defendido por el autor Robert Alexy, responsable de una de las obras clave para la interpretación del alcance de los derechos fundamentales. En su obra[7] Alexy insiste en que, cuando exista la intención de limitar un derecho protegido especialmente por la Constitución, el legislador deberá realizar un esfuerzo extraordinario para justificar la necesidad de esa medida que en origen estaba prohibida. Solo en caso de que se justifique suficientemente su necesidad, se entenderá que estamos ante una medida restrictiva de derechos, pero no vulneradora de los mismos.

1. Derecho a la vida privada

"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones." Así reza el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea. El derecho a la vida privada y familiar ha sido reconocido como derecho fundamental en la gran mayoría de instrumentos internacionales de protección de este tipo de derechos; La Declaración Universal de Derechos Humanos (Artículo 12), el Convenio Internacional de Derechos Civiles y Políticos (Art. 17), el Convenio Europeo de Derechos Humanos (CEDH, en adelante) y por supuesto, la ya citada Carta de los Derechos Fundamentales de la UE.

Este derecho protege a los individuos de la intromisión del estado o de los entes privados en su autonomía personal. Sin embargo, no es un derecho absoluto; "*No podrá haber injerencia por parte de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*[8] Es decir, que es posible imponer límites al

[7] ROBERT ALEXY***, "Teoría de los Derechos Fundamentales"***, Centro de Estudios Constitucionales, Madrid, 1993.

[8] ***Convenio Europeo de los Derechos Humanos***, Tribunal Europeo de Derechos Humanos, Consejo de Europa, Roma el 4 de noviembre de 1950. *"Article 8. Right to respect for private and family life: 1.*

disfrute del derecho a la vida privada, siempre y cuando estos límites se recojan en una norma y su imposición sea controlada por los jueces y tribunales. Así se puede observar en la tradición jurisprudencial del Tribunal Europeo de Derechos Humanos que en múltiples ocasiones se ha referido a la importancia de interpretar este y cualquiera de los derechos enunciados en el Convenio según las condiciones concretas y el momento en que se produzca la supuesta vulneración de los mismos. De este modo, el Convenio sigue adaptándose al momento actual, tomando en consideración los avances tecnológicos en el ámbito de la seguridad nacional e internacional que pueden constituir un nuevo límite al pleno disfrute de los derechos fundamentales que no existía cuando nació el Convenio.

Para que las medidas de vigilancia impuestas por los estados en el ámbito de la seguridad nacional sean válidas, deberán estar contempladas en normas nacionales particularmente precisas, que permitan a los ciudadanos afectados conocer de qué manera podrán las autoridades públicas limitar el ejercicio de sus derechos fundamentales. En los casos excepcionales en que deba imponerse una medida a espaldas del sujeto o sujetos investigados, las autoridades deberán respetar unas mínimas garantías legales a fin de evitar el abuso de poder. Es decir, en los casos tasados en que las autoridades puedan interferir en el pleno disfrute del derecho a la vida privada, por existir circunstancias que lo justifiquen - investigación y persecución del crimen, lucha contra el terrorismo, seguridad nacional - deberán respetarse ciertos límites. La mera existencia de una causa que justifique la limitación de un derecho fundamental, no permite al Estado ignorar completamente estos derechos.

Así se ha pronunciado en numerosas ocasiones el Tribunal Europeo de Derechos Humanos, un ejemplo es el asunto *Marper vs. The United Kingdom*[9] en el que la corte condenó a Reino Unido por haber vulnerado el derecho a la vida privada de dos ciudadanos británicos. Los ciudadanos alegaban la vulneración del Artículo 8 del Convenio por parte de las autoridades del Reino Unido, que continuaban en posesión de

---

Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[9] ***S. & Marper v. United Kingdom*** *(Nº 30562/04 and 30566/04) Tribunal Europeo de Derechos Humanos, Estrasburgo, 4 de diciembre de 2008.*

las huellas dactilares y muestras de ADN que habían obtenido durante los procesos penales a los que se habían sometido los interesados años atrás y que habían concluido con la absolución de ambos y el sobreseimiento de los mismos. El Tribunal reconocía que – tal y como había declarado ya en anteriores procedimientos – el mero almacenamiento de datos o elementos relativos a la vida privada de un individuo suponía una injerencia de lo dispuesto en el Artículo 8 del Convenio. La conservación de esos datos en manos de la autoridad podía estar justificada, por ello el tribunal debía observar concretamente las circunstancias en que dichos datos fueron obtenidos, como fueron procesados y por qué seguían en manos de la autoridad del Reino Unido. Teniendo en cuenta la especial naturaleza de los datos retenidos en este caso – muestras biológicas de ADN y huellas dactilares – el daño que su conservación y uso posterior podría haber causado a los interesados era mayor que si de otro tipo de datos se tratara. Teniendo esto en consideración, la Corte concluyó que la conservación de estas muestras biológicas, una vez concluida la investigación sobre estos sujetos, no entraba entre lo que se considera una medida "*necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales"* en términos del Artículo 8 del Convenio y por lo tanto era innecesaria, desproporcionada y vulneradora del derecho a la vida privada y familiar de los recurrentes.

El interés público y la seguridad nacional constituyen dos de los principios básicos que permiten al estado limitar los derechos de los ciudadanos. Las leyes que regulen el ejercicio y disfrute de los derechos fundamentales, como en España las llamadas Leyes Orgánicas[10], permiten a los estados modular estos derechos en pos de garantizar la seguridad nacional, la prevención del crimen, los principios éticos y morales, la estabilidad económica y por supuesto, el pleno disfrute de los derechos y libertades de los demás.

Como ya hemos mencionado anteriormente, el Artículo 8 del Convenio de Derechos Humanos menciona en su segundo párrafo la posibilidad de restringir el derecho a la vida privada cuando estas restricciones respondan a "una medida necesaria en una sociedad democrática" y sea legítima y proporcionada para la consecución del fin

[10] Constitución Española de 1978, BOE núm. 311 de 29 de diciembre. "*Artículo 81.1*: Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución".

perseguido por la autoridad que impone esa limitación. De esta forma, la aplicación de los medios tecnológicos de vigilancia y seguridad nacional podrá justificarse siempre que respondan a estos principios y que se desarrollen en cumplimiento de la ley y el respeto a la naturaleza misma de los derechos fundamentales.

2. El derecho a la Protección de datos de carácter personal

El derecho a la protección de datos de carácter personal, enunciado en el Artículo 8 de la Carta de los DDFF de la UE, establece que: "*Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan".* En la jurisprudencia del Tribunal de Justicia, este derecho se ha entendido siempre conectado al derecho a la vida privada, recogido en el Art. 7 de la Carta. En el asunto *Promusicae vs. Telefónica de España*[11], el TJUE se enfrentaba a una cuestión prejudicial en la que se le pedía que aclarara el sentido de tres de sus directivas sobre Protección de Datos y Protección de la propiedad intelectual, imprescindibles para el enjuiciamiento en el proceso nacional. La discusión se centraba en la necesidad de ponderar dos derechos especialmente protegidos por el ordenamiento jurídico; el derecho a la propiedad intelectual y la protección de datos de carácter personal. A pesar de que la cuestión prejudicial se centraba en otro asunto, el TJUE se refirió en esta sentencia a esa conexión existente entre el derecho a la protección de datos de carácter personal y el derecho a la vida privada; *"es importante constatar que en la situación controvertida, respecto de la cual el órgano jurisdiccional remitente plantea esta cuestión,* ***interviene, además de los dos derechos mencionados, otro derecho fundamental, a saber, el que garantiza la protección de los datos personales y, en consecuencia, de la intimidad****. (...) De esta forma, la presente petición de decisión prejudicial plantea la cuestión de la necesaria conciliación de las exigencias relacionadas con la protección de distintos derechos fundamentales, a saber, por una parte, el derecho al respeto de la intimidad y, por otra parte, los derechos a la protección de la propiedad y a la tutela judicial efectiva."*

El derecho a la protección de datos se encuentra recogido también en el Art. 8 del Convenio Europeo de los Derechos Humanos del Consejo de Europa, ratificado por los

[11] Sentencia del Tribunal DE Justicia de la UE, ***Productores de España vs. Telefónica de España Sau***, *C-275/06, 29 de enero de 2008, FJ 63.*

28, e indirectamente vinculante para la propia Unión[12]. Así mismo, el ordenamiento jurídico de la UE cuenta con una norma fundamental diseñada para evitar el menoscabo de la protección de datos de carácter personal, frente al movimiento de datos que es una realidad en la era de las telecomunicaciones; la Directiva de Protección de Datos. Esta directiva, traspuesta en España en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, define lo que se entiende por "datos personales" y por "tratamiento de datos personales", entre otros conceptos. Nos interesa recordar estas definiciones a los efectos de entender luego el uso de qué tecnologías puede interferir con el ejercicio y pleno disfrute del derecho a la protección de datos:

En primer lugar, se entiende por "*«datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social."* Y por "*«tratamiento de datos personales»: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción."*[13]

La Directiva establece también las condiciones especiales en que dicho tratamiento de datos puede permitirse, siempre garantizando el respeto a los llamados "datos sensibles"; *"Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o*

[12] Ver *CLARA GONZÁLEZ PUENTE "**El problema de la aplicación del Convenio Europeo de Derechos Humanos y la jurisprudencia de la Corte Europea de Derechos Humanos en el derecho comunitario: la doctrina del caso Bosphorus**". Revista Foro de Derecho Administrativo, Vol. 18, núm. 2, 2015. Editorial Marcial Pons*

[13] ***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.*** Artículo 2. a) y b)

filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad''[14].

III. TECNOLOGÍAS DE VIGILANCIA Y DE DETECCIÓN DE PERSONAS Y LA AFECCIÓN DE LOS DDFF

La tecnología puede ser útil para su uso en el ámbito de la seguridad nacional, pero su uso puede, sin embargo, ser moralmente cuestionable e incluso intrusivo en el ámbito de los derechos fundamentales de los ciudadanos. Además, el uso de la tecnología para la vigilancia y control de la población puede plantear cuestiones éticas no cubiertas por la ley o bien, aquellos usos que parecen moralmente justificables en un primer momento pueden ser incompatibles con los derechos humanos reconocidos por cada estado.

Las tecnologías que vamos a estudiar en este proyecto han sido seleccionadas en virtud de la relevancia de su uso en el ámbito de la lucha contra el terrorismo, el crimen organizado y el mantenimiento de la seguridad nacional e internacional.

Los derechos fundamentales que pueden verse directamente limitados por estas tecnologías son, principalmente, el derecho a la protección de la vida privada y el derecho a la protección de datos de carácter personal. A pesar de la innegable conexión que existe entre ambos derechos, el derecho a la protección de datos de carácter personal se concibe cada vez más con un derecho autónomo. Así queda recogido en la Carta de Derechos Fundamentales de la UE, en la que el derecho a la protección de la vida privada y los datos de carácter personal se recogen en dos artículos consecutivos; Artículos 7 y 8 de la Carta. [15]

---

[14] ***Directiva de Protección de Datos***, Artículo 8. 1. Cit. Nota 13.

[15]**Carta de los Derechos Fundamentales de la Unión Europea** (2000/C 364/01)**, Niza 7 de diciembre de 2000:** *Artículo 7 Respeto de la vida privada y familiar*: *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones."* Artículo 8 Protección de datos de carácter personal:*"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedar sujeto al control de una autoridad independiente."*

El concepto de vida privada se refiere tanto a la integridad física como psíquica de cualquier persona tanto en su vida íntima como en su desarrollo en sociedad; elementos como la orientación y vida sexual o la identificación del género entran dentro de este derecho fundamental. También se protege en el Artículo 8 de la Carta el derecho al desarrollo personal, el derecho a establecer relaciones con otros seres humanos y a la autodeterminación.

El derecho a la protección de datos de carácter personal se refiere a la protección de los intereses individuales y libertades de los individuos, cuando se accede y se maneja su información personal. El problema viene al determinar concretamente si todos los datos personales entran dentro del concepto de vida privada y merecen por lo tanto una especial protección.

Sobre este hecho se pronunció precisamente el Tribunal de Primera Instancia de la UE, en el asunto ***Bavarian Lager vs. European Comission***, en noviembre de 2007, diciendo: *"Procede también subrayar que el hecho de que, conforme a la jurisprudencia del Tribunal Europeo de Derechos Humanos, el concepto de «vida privada» sea amplio, y el derecho a la protección de datos personales pueda constituir uno de los aspectos del derecho al respeto de la intimidad, no significa que todos los datos personales entren necesariamente en el concepto de «intimidad». A fortiori, no todos los datos personales pueden, por su naturaleza, suponer un perjuicio para la intimidad del interesado. En efecto, en el trigésimo tercer considerando de la Directiva 95/46, se hace referencia a los datos que por su naturaleza pueden atentar contra las libertades fundamentales o la intimidad y que no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito, lo que indica que no todos los datos tienen la misma naturaleza. Tales datos sensibles pueden incluirse en aquéllos a los que se refiere el artículo 10 del Reglamento nº 45/2001, relativos al tratamiento de categorías particulares de datos como los que revelan el origen racial o étnico, las convicciones religiosas o filosóficas, o los datos relativos a la salud o a la sexualidad."*

Dejando de un lado el derecho a la protección de la vida privada y a la protección de datos de carácter personal, otros muchos derechos pueden verse afectados directamente por la aplicación de las nuevas tecnologías en el ámbito de la seguridad nacional, incluyendo la libertad de pensamiento, de movimiento, libertad religiosa y de conciencia, libertad de expresión, no discriminación…

1. Circuitos cerrados de televisión y fotografía digital

Los circuitos cerrados de televisión (*Closed Circuit Television* o CCTV en inglés) son sistemas de video vigilancia en los que, cada una de las cámaras integradas en el circuito transmite la señal captada a un número limitado de monitores, conectados de forma particular al circuito. Gracias a los avances tecnológicos de los últimos años, este tipo de vigilancia ha alcanzado un nivel de definición de la imagen tal, que permite a quienes la controlan identificar, rastrear y definir los objetos dentro del campo de visión. Los actuales sistemas de análisis de imagen informáticos permiten, además detectar patrones anormales de conducta entre una multitud de personas.

Además, los Circuitos Cerrados de Televisión, también conocidos como CCTV, por sus siglas en inglés, están equipados con un complejo sistema de reconocimiento facial que puede reconocer a una persona de forma automática en cualquier documento videográfico.

A) Descubierto

Los circuitos cerrados de video vigilancia son cada vez más comunes en el ámbito de la seguridad privada de empresas y zonas residenciales. En este ámbito, las cámaras de seguridad no deben estar orientadas en la vía pública salvo en casos excepcionales. Sí existe, sin embargo, un tipo de video vigilancia en la vía pública reservado al uso exclusivo de los Cuerpos y Fuerzas de Seguridad de los Estados miembros de la Unión. En España esta ley es la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. En su artículo 1 se establece el objeto de esta ley;

> *"1. La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.*
>
> *Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de*

respetarse ineludiblemente en las sucesivas fases de autorización, grabación y uso de las imágenes y sonidos obtenidos conjuntamente por las videocámaras.

2. Las referencias contenidas en esta Ley a videocámaras, cámaras fijas y cámaras móviles se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta Ley."

Se establecen una serie de criterios de proporcionalidad, que deberán estudiarse a la hora de decidir si es necesario o no el uso de estos dispositivos en la vía pública. De este modo, se tendrá en cuenta la salvaguarda de la seguridad ciudadana, la protección de los edificios y zonas de interés público, la necesidad de evitar la comisión de ciertos delitos, y otros criterios que serán valorados por una Comisión ad hoc, presidida por un Magistrado, previa a la autorización gubernativa.

Como ya sabemos, los derechos de privacidad y protección de datos no son ilimitados. La colocación de cámaras de video vigilancia en espacios públicos, cuando son visibles y han sido colocadas por una autoridad, no suele considerarse vulneradora de estos derechos. La captación de imágenes que muestren el movimiento de los individuos en un lugar público no tiene por qué entenderse vulnerador del derecho a la vida privada. Otra cuestión será que esas imágenes lleguen a ser procesadas y utilizadas para identificar a algunas de las personas que hayan sido grabadas. Sin embargo, al evaluar la intromisión de esta práctica en los derechos fundamentales mencionados, los tribunales y, especialmente el TJUE, han considerado que se trata de prácticas muy levemente intrusivas. La doctrina y la jurisprudencia europea consideran que, aunque el derecho a la vida privada y la protección de datos también deben ser respetados en la vía pública, su ejercicio en este contexto es mucho más leve[16]. Cualquier persona puede ser vista

[16] ***P.G. y J.H. vs. Reino Unido. Nº 44787/98***, TEDH, Estrasburgo, 25 septiembre de 2001: "57. *There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures affected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method"*

cuando se encuentre fuera de su hogar o de un recinto privado, por lo que la inclusión en este contexto de un dispositivo CCTV no tiene por qué suponer una vulneración mayor de los derechos enunciados a la que se produce por el simple hecho de caminar por la vía pública pudiendo ser observado por ciudadanos civiles, cámaras de seguridad privadas[17] o agentes de policía. Esta reflexión se hace sin perjuicio de que cualquier medida de vigilancia que se tome, aunque sea perfectamente visible por los ciudadanos, deberá estar fundada en una ley que le sirva de base.

En la legislación europea volveríamos a referirnos a la Directiva de Datos, que también regula expresamente la instalación privada de cámaras de video vigilancia por particulares y empresas y, como la LO 4/1997, prohíbe que dichas cámaras graven la vía pública y a los viandantes sin su consentimiento. El legislador europeo considera que las imágenes captadas por las cámaras de CCTV pueden ser consideradas como material sensible en el ámbito de la protección de datos de carácter personal. Las cámaras pueden grabar la imagen de una persona, permitiendo a quien las observa conocer datos como la raza, la edad aproximada, la religión o la orientación sexual de una persona, de forma que se esté produciendo con esta grabación una intromisión directa en aspectos íntimos de la vida de una persona sin su permiso.

Sin embargo, la Directiva no se aplica al tratamiento de datos que realice una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Sobre este extremo se pronunció el TJUE en la sentencia del *Asunto Rynes vs. Úrad*[18] en 2014.

El señor Rynes había sufrido robos en su vivienda en varias ocasiones, por lo que se decidió a instalar un sistema de cámaras de video vigilancia privada en su hogar. Algunas de estas cámaras captaban, no solo el interior de la vivienda, sino también la entrada de la misma, la vía pública e incluso, la vivienda de en frente. Al poco tiempo de instalarlas, se produjo de nuevo un intento de robo en la casa del señor Rynes. Gracias a las cámaras de seguridad, los responsables fueron identificados y se inició un proceso penal contra ellos. Uno de los investigados por el robo denunció que la captación de su imagen en la vía pública - la que había servido concretamente para identificarle como responsable del robo - suponía una violación de su derecho a la protección de datos de carácter personal y, por ende, una obtención ilícita de esa prueba

[17] Se analiza este asunto a continuación

[18] Sentencia del Tribunal de Justicia de la Unión Europea ***František Ryneš / Úřad pro ochranu osobních údajů*** *C-212/2013,* 11 de diciembre de 2014

de cargo, que no debía ser utilizada. Ante la duda de si la actividad realizada por el señor Rynes constituía un tratamiento de datos al que no se aplicaba la Directiva por haber sido efectuada la grabación por una persona física en el ejercicio de actividades exclusivamente personales, planteó el Tribunal Supremo de la República Checa una cuestión prejudicial al TJUE.

En la sentencia, el TJUE definía de nuevo el concepto de datos personales, "*toda información sobre una persona física identificada o identificable"* y reconocía que, efectivamente, "*la imagen de una persona grabada por una cámara constituye un dato personal porque permite identificar a la persona afectada".* Con respecto a si el tratamiento de las imágenes grabadas se podía entender como uso personal y doméstico, el tribunal declaraba que procedía aplicar una interpretación estricta de esta excepción.

La instalación de cámaras de video vigilancia doméstica en el espacio público, estaría abarcando un terreno no reservado a la esfera "personal y doméstica", por lo que en este sentido supondría una intromisión en los derechos de las terceras personas que transitaran dicha vía. A pesar de ello, es necesario proteger también el interés legítimo del señor Rynes por proteger sus bienes, su vida y la de su familia. Con la instalación del sistema de CCTV, el señor Rynes intentaba evitar un nuevo robo y allanamiento de su hogar. Este interés legítimo necesitaba, para ser efectivo, de la colocación de las cámaras en la entrada de la vivienda con el resultado inevitable de que se captarían imágenes de la vía pública y de quienes transitaran por ella.

El TJUE se pronunció, tras ponderar los derechos fundamentales en juego, en el siguiente sentido;

- El tratamiento de datos personales podrá hacerse sin el consentimiento del interesado cuando dicho tratamiento sea necesario para satisfacer el interés legítimo de quien lo realiza, en este caso, la protección de la vida familiar y personal del señor Rynes.
- No será necesario informar a los afectados por el tratamiento de sus datos cuando dar tal información sea imposible o requiera esfuerzos desproporcionados. El señor Rynes no podía haber informado a todas las personas que transitaban la vía pública de que sus imágenes estaban siendo

recogidas en una cámara de seguridad, como tampoco podía - lógicamente - informar a los ladrones de la instalación de la vídeo cámara.

- Finalmente, se remitía el TJUE a las leyes nacionales de transposición, diciendo que éstas podrían limitar el alcance de los derechos previstos en la Directiva de Datos, para garantizar la prevención e investigación de los delitos y la protección de los derechos de los ciudadanos.

La ley española sigue la línea del pronunciamiento del TJUE en este asunto, y recoge en su Artículo 4 la posibilidad de que las cámaras de CCTV graben imágenes de la vía pública en las circunstancias excepcionales enunciadas en la Sentencia Rynes vs. Úrad;

> *"1. Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras. 2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal. 3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida".*

En esta misma línea encontramos otra sentencia, en esta ocasión del Tribunal Europeo de Derechos Humanos, que aporta un nuevo enfoque sobre el uso de cámaras de vigilancia en la vía pública. En este asunto[19] el demandante, Don José Luis de la Flor Cabrera de nacionalidad española, solicitaba el amparo del TEDH de Estrasburgo alegando la vulneración de su derecho al honor, a la intimidad personal y familiar y a su propia imagen. Don José Luis había sido arrollado por un vehículo mientras circulaba en bicicleta por Sevilla en 1997, por lo que había promovido la correspondiente acción civil por daños contra el conductor del vehículo y la compañía aseguradora, alegando

[19] ***De la Flor Cabrera vs. Reino de España***, nº 10764/09, TEDH, 27 de mayo de 2014

que padecía desde el accidente una neurosis post-traumática que le impedía conducir vehículo alguno.

Ante estas declaraciones, la compañía aseguradora presentó una grabación en vídeo en la que se veía a Don José Luis conduciendo una moto, desmintiendo así la existencia del miedo alegado. Estos vídeos habían sido grabados por un detective privado contratado por la compañía aseguradora y con total desconocimiento del demandante. Las pruebas fueron aceptadas por el Juzgado, que condenó a la aseguradora a pagar una indemnización mucho menor de la solicitada por Don José Luis, por lo que éste acudió al TEDH.

En su razonamiento, el Tribunal de Estrasburgo comenzaba por reconocer que el derecho a la "vida privada", recogido en el Artículo 8 del Convenio Europeo de Derechos Humanos, engloba tanto la integridad física y moral de la persona, como los elementos de la identidad del individuo, que tiene derecho a decidir qué información personal revelar y cual no. Haciendo referencia a un pronunciamiento anterior del propio tribunal, el asunto Schüssel vs. Austri de 2002, el TEDH reconocía que la publicación de imágenes y fotografías de la vida privada de cualquier sujeto era un acto de interferencia en su derecho a la vida privada, incluso en caso de que ese sujeto fuera un personaje público. Por lo que se reconoce el derecho a la protección de la propia imagen y al control de la difusión de la misma, que no solamente se ejerce de manera personal, sino que debe estar garantizada también por los poderes públicos. El artículo 8 del CEDH requiere del compromiso de los Estados Miembros, que se obligan positivamente a respetar la vida privada y familiar de los ciudadanos. Los Estados Miembros tendrán la potestad de establecer un equilibrio entre el respeto de los derechos privados reconocidos y la existencia de un interés público que justifique la divulgación de ciertos datos de carácter personal.

Sin embargo, el Tribunal continuaba diciendo que en el presente asunto no se estaba ante la difusión pública de imágenes de la vida privada de Don José Luis, sino ante su uso en un procedimiento judicial. Las imágenes grabadas no estaban destinadas a ser publicadas, sino que iban a ser utilizadas como medio de prueba en un proceso civil. Los vídeos se habían grabado en la vía pública, cuando el demandante se encontraba realizando una actividad de desplazamiento que podía haber sido presenciada por cualquier persona. Una agencia de detectives privados, respetuosa de las leyes

nacionales sobre seguridad privada, había grabado las imágenes que tenían la intención de contribuir al debate judicial, aportando fuerza a los argumentos de la compañía aseguradora, que pretendía probar que la incapacidad para la conducción del demandante era una falsedad. Siendo esta supuesta incapacidad uno de los elementos clave del asunto civil, cualquier prueba que arrojara luz sobre el asunto se consideraba necesaria, siempre y cuando hubiera sido obtenida legítimamente. El tribunal consideró que así había sido, igual que anteriormente lo había hecho el juez nacional. Estrasburgo puso por delante, en esta ocasión, el interés público de garantizar el acceso a los medios de prueba de las partes frente al derecho a la vida privada, fallando en contra de Don José Luis.

Para continuar analizando el uso de dispositivos de vídeo y su interferencia en los derechos fundamentales, es necesario ir más allá. ¿Qué ocurriría si nos situamos en la esfera de la empresa privada y los derechos de los trabajadores? ¿Puede un empresario colocar cámaras en un centro de trabajo libremente? ¿Debe avisar previamente a sus trabajadores?

Para analizar este hecho acudimos al Derecho Interno, concretamente a la línea jurisprudencial seguida por nuestro Tribunal Supremo.

El Texto Refundido del Estatuto de los Trabajadores establece en su artículo 20.3 que; "*El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad."* Es decir, dota al empresario de una potestad de control bastante extensa cuyo límite es la dignidad de los trabajadores y el respeto a sus derechos fundamentales.

Sin embargo, como venimos analizando, el pleno disfrute de los derechos fundamentales puede verse afectado o limitado en circunstancias especiales, como sería en medio de una relación contractual laboral, en la que el empresario contratante tiene la capacidad de controlar y limitar la libre actuación de sus empleados durante la prestación de servicios.

Sobre este hecho se ha pronunciado el Tribunal Constitucional Español en la Sentencia de 3 de marzo de 2016[20], que ha aclarado la doctrina constitucional en relación con el uso de cámaras de video vigilancia en la empresa.

En este asunto, una empleada de una tienda de moda había sido despedida disciplinariamente por haber sido grabada sustrayendo dinero de la caja registradora. Las imágenes se obtuvieron a partir de las cámaras de seguridad instaladas en la tienda. No se había anunciado previamente a los trabajadores sobre la instalación de las cámaras, pero sí se habían colocado símbolos distintivos en el local y a la entrada del comercio. Ante este despido, la afectada presentó varios recursos hasta llegar al amparo del alto tribunal.

El TC reconocía efectivamente que el tratamiento de los datos personales solamente es posible con el consentimiento de sus titulares, salvo que exista habilitación legal para que los datos puedan ser tratados sin dicho consentimiento. En el ámbito laboral el consentimiento del trabajador pasa, como regla general, a un segundo plano pues se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes. Esto abarca las obligaciones derivadas del contrato de trabajo, por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Sin embargo, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

Ahora bien, aunque no sea necesario el consentimiento en los casos señalados, el deber de información sigue existiendo, pues permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición cuando la finalidad del tratamiento de datos no sea el desarrollo y control de la relación contractual.

La ausencia o deficiencia de información en los supuestos de video vigilancia laboral exige la ponderación en cada caso de los derechos y bienes constitucionales en conflicto; es decir, el derecho a la protección de datos del trabajador y el poder de

[20] ***Sentencia del Pleno del Tribunal Constitucional 39/2016, de 3 de marzo de 2016.*** Recurso de amparo 7222-2013.

dirección y control del empresario que es imprescindible para el buen funcionamiento de la empresa.

En este caso, el trabajador conocía que en la empresa se había instalado un sistema de control por video vigilancia, sin que se hubiera especificado la finalidad exacta que se le ha asignado a ese control. Lo importante será determinar si el dato obtenido se ha utilizado para el control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados, o al menos a informar debidamente de la finalidad perseguida con la instalación de los dispositivos de vídeo vigilancia.

La falta o la insuficiencia de información deberá someterse, con carácter previo, al juicio de proporcionalidad que determinará en cada supuesto si hay omisión de la información debida. Así quedó reflejado en una Sentencia anterior de la Sala de lo Social del TS en mayo de 2014[21], en la que el TS declaraba nulo el despido de una cajera de supermercado que había sido grabada por las cámaras de seguridad evitando el escaneo de varios productos en beneficio de los compradores. La empleada recurrió el despido disciplinario alegando la vulneración de su derecho fundamental a la propia imagen y protección de datos de carácter personal, pues entendía que la obtención de las imágenes que constituían la prueba de la conducta sancionada había sido ilegal y contraria a sus derechos constitucionales.

La empresa alegaba de contrario que las cámaras habían sido instaladas respetando la normativa vigente y con previo aviso a los trabajadores, a quienes se había anunciado la instalación de cámaras para evitar el robo de productos por parte de los clientes. He aquí el quid de la cuestión; la empresa cometió un error al no informar previamente a los trabajadores de que las cámaras de seguridad también les controlaban a ellos en sus puestos de trabajo. En ningún momento se informó de la posibilidad de utilizar las imágenes grabadas como prueba para imponer sanciones disciplinarias a los trabajadores, sino como dispositivos de control de la seguridad del local y de evitación de robos por parte de terceros. Según el TS, "*era necesaria además la información*

[21] ***Sentencia de la Sala de lo Social del Tribunal Supremo de 13 de mayo de 2014***, Recurso de Unificación de Doctrina número 1685/2013

previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida" y, además, *"la ilegalidad de la conducta empresarial no desaparece por el hecho de que la existencia de las cámaras fuera apreciable a simple vista"*. Por lo que el tribunal aceptó la tesis de la trabajadora y obligó a la empresa a readmitirla, considerando el despido nulo.

B) Encubierto

Los derechos fundamentales de los ciudadanos son especialmente vulnerables cuando se realiza este tipo de vigilancia. La instalación de cámaras de video vigilancia ocultas en lugares públicos es una técnica altamente intrusiva en la esfera de los DDFF de los ciudadanos. Del mismo modo, la instalación de dispositivos ocultos en establecimientos privados con el objeto de controlar a sujetos sospechosos de la comisión de algún delito, requiere también de un especial control de legalidad.

Mientras que el uso de estos dispositivos en la vía pública, siempre que sean visibles a los ciudadanos, está permitido a las autoridades sin considerarse una práctica vulneradora de los derechos de privacidad y protección de datos, el uso encubierto de estos dispositivos es más problemático.

El TEDH se pronunció al respecto en el año 2003, en el asunto *Peck vs. United Kingdom*[22]. En agosto de 1995, la policía evitó el intento de suicidio que el señor Geoffrey Peck iba a cometer en plena calle en Brentwood, Reino Unido. La policía acudió al lugar alertada por las imágenes captadas por una cámara de vigilancia vial, situada en un cruce cercano a donde el señor Peck se encontraba. El problema vino cuando un tiempo después las imágenes del suceso fueron divulgadas públicamente en la prensa, anunciando que gracias al uso de las cámaras de seguridad vial se había podido evitar un suceso potencialmente peligroso. El señor Peck acudió a la Corte alegando la vulneración de su derecho a la vida privada, no por el hecho de que las imágenes hubieran sido grabadas y remitidas a la policía, hecho que reconocía le había salvado la vida, sino por la divulgación posterior de dichas imágenes. La corte reconoció en su razonamiento que, efectivamente, la divulgación de las imágenes del

[22] ***Peck vs. Reino Unido***, nº 44647/98, TEDH, enero de 2003

señor Peck en la prensa amarilla había supuesto una vulneración de su intimidad y privacidad. La identidad del demandante no fue correctamente protegida; no se le tapó la cara ni se limitó de forma alguna la circulación pública de las imágenes. Como consecuencia, el señor Peck fue reconocido por numerosos familiares, amigos y vecinos de Brentwood, quedando su intimidad expuesta a la generalidad. La Corte dio la razón al señor Peck y condenó a Reino Unido, estableciendo a su vez una línea roja en el uso de la información obtenida por las cámaras de vigilancia policial públicas:

- El material obtenido por las cámaras de vigilancia policial ocultas en lugares públicos no puede ser utilizado de manera intrusiva y no prevista en las leyes
- El referido material no podrá ser divulgado ni difundido públicamente, su uso se limitará al ámbito de la investigación policial.

2. Control de dispositivos de audio

Los dispositivos de audio utilizados en los sistemas de vigilancia, como los micrófonos ocultos o las grabadoras de sonido, son dispositivos de pequeño tamaño que pueden ensamblarse en cualquier tipo de objeto cotidiano o en cualquier dispositivo móvil. Estos pequeños aparatos captan el sonido gracias a los sensores de audio que son capaces de transformar la señal sonora emitida en una señal eléctrica que queda grabada y es almacenada en el receptor que la transforma en una señal de audio analógica.

Este tipo de dispositivos de intervención de las comunicaciones pueden, por su diminuto tamaño, servir a cualquier tipo de propósito, siendo incluso posible introducirlos en un teléfono móvil normal, para poder rastrear tanto las comunicaciones telefónicas, como el movimiento de cualquier individuo mediante una señal GPS.

Tanto en derecho europeo como en el ámbito nacional, el uso legítimo de este tipo de técnicas requiere de la existencia de una normativa detallada y precisa que lo respalde. Según el ya citado Artículo 8 del Convenio Europeo de los Derechos Humanos, *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia (...) no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho (vida privada y familiar) sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la*

moral, o la protección de los derechos y las libertades de los demás". Es decir, que además de previsión normativa, la intervención de las comunicaciones debe ser necesaria para evitar la comisión de un delito o para garantizar la seguridad pública.

El Tribunal Europeo de Derechos Humanos ha interpretado que el control de dispositivos de audio es una práctica claramente vulneradora del derecho a la privacidad y a la protección de datos, por lo que una medida de este tipo debería fundarse siempre en una ley clara, precisa y detallada. A este respecto se pronunciaba el TEDH en el Asunto Vetter vs. France, en 2005[23], en el que un ciudadano francés acudía al tribunal alegando la vulneración del derecho a la vida privada regulado en el citado Artículo 8. El afectado aducía que había sido condenado a veinte años de prisión, en base a unas pruebas que habían sido ilícitamente obtenidas y que vulneraban claramente sus derechos fundamentales.

La policía francesa, sospechando de la culpabilidad de Vetter, había colocado en su domicilio varios dispositivos de escucha y había obtenido declaraciones que comprometían seriamente al recurrente. Vetter alegaba que no había base jurídica que fundamentara la colocación de los dispositivos de escucha en el Código Penal francés, y que su colocación injustificada había vulnerado gravemente los derechos enunciados en el Art. 8 del CEDH. El tribunal francés alegó a este respecto que la colocación de los dispositivos se justificaba en la aplicación analógica de los artículos sobre intervención de las comunicaciones telefónicas del Código Penal francés.

Ante estas alegaciones, el TEDH no pudo más que dar la razón al recurrente reconociendo que "*una medida de investigación tan intrusiva no puede fundamentarse en normas generales, principios o en la aplicación analógica de otros preceptos similares. Aunque pueda ser posible dicha extrapolación no conlleva una certeza legal suficiente en el presente caso".* Para el tribunal es imprescindible que, en el ámbito de las medidas de investigación tecnológicas que puedan interferir con el pleno disfrute de los derechos fundamentales, existan en los estados miembros normas concretas en las que se especifiquen los motivos que justifican la aplicación de una medida de investigación de este tipo. Estas normas deberán contemplar de forma exhaustiva qué delitos podrán justificar la toma de alguna de estas medidas de investigación, qué

[23] ***Vetter vs. France, nº 59842/00***. TEDH, 31 de mayo de 2005

límites temporales o subjetivos deberán ser tenidos en cuenta o cuál deberá ser el tratamiento posterior de la información que se obtenga mediante su aplicación.

A pesar de la existencia de dichas normas, es innegable que la captación y grabación de cualquier tipo de sonido en el domicilio mediante el uso de dispositivos de audio tiene un grave impacto sobre los derechos fundamentales. El derecho a decidir qué información personal compartir y con quién compartirla es parte del contenido básico y medular del derecho a la vida privada. Este derecho se desarrolla plenamente en el domicilio de la persona investigada o en cualquier otro lugar íntimo equiparable. La colocación de dispositivos de grabación en la vivienda de un sujeto se considera mucho más intrusiva que, por ejemplo, el seguimiento o rastreo vía GPS, pues revela información concreta sobre las opiniones, sentimientos y conductas que una persona desarrolla en la intimidad de su hogar. Es por ello que este tipo de medidas deberán tomarse solo bajo las circunstancias excepcionales que ya hemos señalado anteriormente, y siempre prestando una especial atención a los derechos fundamentales de las personas cuya vigilancia se pretenda.

Pero, ¿qué ocurre cuando las grabaciones no se obtienen en el domicilio del afectado, sino en la vía pública, en un vehículo privado, en cualquier medio de transporte público o en el centro de trabajo? Tal y como reconoció el Tribunal Europeo de Derechos Humanos en el *Asunto Uzun vs. Alemania*[24], la colocación de dispositivos grabadores de audio es, por regla general, susceptible de ser más intrusivo en los derechos fundamentales de los individuos que otros medios de vigilancia (en la sentencia el Tribunal lo compara con el seguimiento vía GPS), ya que revelan un mayor número de datos relativos a la conducta, opiniones y sentimientos de los sujetos objeto de la investigación, por lo que, si no se respetan los principios de proporcionalidad y legalidad referidos, puede producirse una vulneración de los derechos recogidos en los Artículos 7 y 8 del Convenio Europeo de Derechos Humanos.

Esto no implica que no puedan utilizarse bajo ninguna circunstancia las grabaciones de sonido como prueba en un proceso judicial. Para explicar esta circunstancia acudimos a una sentencia dictada por el Tribunal Supremo en 2014[25].

[24] ***Uzun v. Germany, Rec. 35623/05. TEDH***, 2 de diciembre de 2010.
[25] ***Sentencia de la Sala de lo Civil del Tribunal Supremo Núm. 678/2014 de 20 de noviembre de 2014***.

En el asunto, una trabajadora había grabado la conversación en la que su jefe le comunicaba, antes de entrar en la oficina, que estaba despedida. Posteriormente, la trabajadora – parte demandada en esta sentencia – había intentado utilizar dicha grabación como prueba en el juicio por despido improcedente contra la empresa. La empresa impugnó la referida prueba, alegando que había sido obtenida de forma ilícita, sin el previo consentimiento de la otra parte y que su difusión vulneraba el derecho a la vida privada, el secreto de las comunicaciones y la protección de datos personales del empleador.

Sin embargo, el Juzgado de Primeria Instancia desestimó las pretensiones del demandante, reconociendo el valor probatorio y la legitimidad de la grabación impugnada. Posteriormente fue el propio Tribunal Supremo quien desestimó las alegaciones del empleador, refiriéndose en primer lugar a "*la inexistencia de una intromisión ilegítima en el derecho a la intimidad personal del demandante"*, al tratar la conversación grabada de temas exclusivamente laborales que, por su naturaleza, no revelaban ningún dato de carácter privado ni manifestaban aspectos íntimos de la vida del demandante. Además, quedaba probado que el destino de la grabación realizada era su uso como prueba en un proceso judicial y no su difusión o comunicación pública, por lo que el tribunal descartaba que se hubiera producido la vulneración de los derechos a la vida privada y la protección de datos.

En cuanto a la vulneración del derecho a la privacidad de las comunicaciones, el tribunal sentenciaba; *"sea cual sea el ámbito objetivo del concepto de «comunicación», la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados) ajenos a la comunicación misma, de tal manera que no hay «secreto» para aquel a quien la comunicación se dirige ni implica contravención de lo dispuesto en el Art. 18.3 de la Constitución la retención por cualquier medio del contenido del mensaje. Dicha retención (la grabación en el presente caso) podrá ser, en muchos casos, el presupuesto fáctico para la comunicación a terceros, pero ni aun considerando el problema desde este punto de vista puede apreciarse la conducta del interlocutor como preparatoria del ilícito constitucional, que es el quebrantamiento del secreto de las comunicaciones."* Es decir, la vulneración de este derecho no tiene cabida si el sujeto demandado es interlocutor de las "comunicaciones" supuestamente reveladas. Aquí estaríamos haciendo referencia a

la doctrina sentada en una sentencia anterior de nuestro Tribunal Supremo[26] en la que se distinguía que; *"quien graba una conversación de otros atenta, independientemente de toda otra consideración, al derecho reconocido en el art. 18.3 de la Constitución; por el contrario, quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado."* Haciendo una importante distinción en la legitimidad de una prueba de este tipo cuando el sujeto que graba la conversación participa en la misma o cuando es un mero espectador que graba un mensaje sin ser destinatario del mismo.

3. Inspección del equipaje con Rayos X

Los controles de seguridad sobre el equipaje son una práctica habitual y estandarizada, especialmente en caso de que dicho equipaje vaya a viajar en avión. Tradicionalmente, las máquinas de rayos X han sido utilizadas para localizar e identificar instrumentos metálicos dentro del equipaje de pasajeros. Actualmente todavía se utiliza este tipo de detección de metales, aunque gracias a los avances tecnológicos, estas máquinas de rayos X se utilizan combinadas con otros equipos de detección, especialmente de detección de sustancias líquidas, inflamables e incluso explosivas.

Los escáneres de última generación son capaces de detectar una mayor variedad de materiales explosivos utilizando ondas de luz capaces de examinar contenedores sellados en busca de material explosivo.

En primer lugar, es necesario tener en cuenta que este tipo de actuación - que busca garantizar la seguridad en lugares de especial interés, como son las estaciones y aeropuertos, que atraviesan diariamente millones de personas y de mercancías de diversa naturaleza – es por sí misma una práctica que traspasa los límites de la privacidad. Toda persona que pretende realizar un viaje y que transporta algunos de sus bienes personales debería tener derecho a decidir quién puede ver aquello que transporta. Sin embargo, el derecho a la intimidad no es absoluto. La imposición de límites a la vida privada y la intimidad debe estar, como ya hemos resaltado anteriormente, especialmente previsto en una norma. Además, estos límites deben respetar siempre los principios de necesidad y proporcionalidad, pudiendo incurrir en

[26] ***Sentencia de la Sala de lo Penal del Tribunal Supremo, Núm. 45/2014*** de 7 de febrero de 2014

una violación injustificada de derechos, en caso de ser limitaciones no justificables en relación a dichos principios.

En enero de 2015 entraba en vigor un nuevo reglamento europeo que reforzaba la seguridad en los aeropuertos, aumentando las medidas de control del equipaje de los usuarios[27]. Esta nueva norma respondía al aumento de ataques terroristas en Europa desde la autoproclamación del grupo terrorista insurgente Dáesh (Estado Islámico, en su acrónimo inglés) en junio de 2014. En la exposición de motivos del Reglamento 187/2015, la Comisión justifica la ampliación de las medidas de seguridad como sigue:

> *"Datos recientes han demostrado que nuevos modos de ocultación de artefactos explosivos improvisados están siendo desarrollados por terroristas con el fin de contrarrestar las medidas de seguridad aérea existentes en relación con la inspección del equipaje de mano. (2) Por consiguiente, deben modificarse determinadas medidas de seguridad aérea establecidas en el Reglamento (UE) no 185/2010 de la Comisión, a fin de mejorar la mitigación de la amenaza de artefactos explosivos improvisados ocultos en el equipaje de mano. (3) Las modificaciones deben puntualizar las especificaciones técnicas para la inspección del equipaje de mano mediante el uso de sistemas de detección de explosivos. (4) Las modificaciones también deben permitir la inspección del equipaje de mano que contenga ordenadores portátiles y otros artículos eléctricos de gran tamaño en determinadas condiciones. (5) Por consiguiente, procede modificar el Reglamento (UE) no 185/2010 en consecuencia. (6) El presente Reglamento debe entrar en vigor lo antes posible, con vistas a minimizar los riesgos para la seguridad aérea. (7) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité de Seguridad de la Aviación Civil."*

En su virtud, las medidas de control de equipaje mediante el uso de escáneres de rayos x en estaciones, aeropuertos y edificios públicos, entrarían dentro de la legalidad siempre que se cumplan las prescripciones recogidas en este Reglamento.

Es cierto que otros derechos pueden verse afectados cuando un agente autorizado revisa algo tan privado como el equipaje de una persona. Una maleta o bolsa de viaje puede contener objetos religiosos, publicaciones de contenido político o elementos que revelen

[27] ***REGLAMENTO DE EJECUCIÓN (UE) 2015/187 DE LA COMISIÓN de 6 de febrero de 2015*** por el que se modifica el Reglamento (UE) no 185/2010 en lo que se refiere a la inspección del equipaje de mano

la orientación y las prácticas sexuales de los individuos. La revelación de este tipo de elementos puede implicar la violación de la libertad de expresión, libertad religiosa e ideológica y puede también desembocar en un trato discriminatorio por parte de los agentes de seguridad que realicen el control del equipaje, especialmente en países políticamente más represivos.

Para que esto no se produzca, el control de seguridad debe limitarse a comprobar que el sujeto no lleva consigo drogas, explosivos, armas o cualquier otro objeto catalogado como peligroso. Para determinar la legitimidad de la intrusión, tendremos que tener en consideración el nivel de vulneración de derechos frente a la necesidad de aplicar la medida de seguridad. Si, en última instancia, la necesidad de evitar un daño mayor justifica la vulneración de derechos, estaremos ante una medida de seguridad justa.

4. Instrumentos de análisis de datos

Las herramientas de análisis de datos informáticos se emplean mucho en la lucha contra el crimen organizado y el terrorismo. Examinan voluminosos sets de datos existentes en internet. Dentro de este tipo de análisis se ha producido un gran desarrollo en los últimos años. Por ello, se han desarrollado sistemas novedosos de análisis de datos en Redes Sociales; capaces de realizar un estudio estadístico de los patrones de comunicación en los distintos grupos en función de su edad, origen, nivel económico, estudios…

Aunque el uso de este tipo de software de análisis de datos por las autoridades nacionales puede ser proporcionado en la lucha contra el crimen organizado y la lucha contra el terrorismo, también encontramos numerosas prácticas totalmente vulneradoras de derechos fundamentales. Las agencias estatales de inteligencia recurren en ocasiones al uso indiscriminado de estas medidas de investigación, haciendo caso omiso de la barrera invisible que debería existir cuando entran en juego los derechos a la intimidad, la vida privada y la protección de datos de carácter personal.

En 2015, una compañía italiana de tecnología de la información o *IT* (*Information Technology*, según las siglas en ingles), que se dedicaba a la venta de herramientas de vigilancia e intrusión ofensiva de las comunicaciones, sufrió un ataque cibernético que filtró una gran cantidad de datos secretos pertenecientes a la compañía y a algunos de

sus clientes por todo el mundo. Muchos de estos datos fueron publicados en internet, revelando que algunos de los clientes más importantes de la empresa de *hacking* (o piratería informática) eran las agencias de inteligencia y órganos de seguridad de estados de todo el mundo. Gracias a esta filtración salió a la luz la naturaleza de este tipo de *software* de vigilancia, capaz de controlar dispositivos electrónicos y bases de datos a distancia sin ser percibido. Al descubrirse que este software había sido vendido a estados y organizaciones gubernamentales, surgió la visión crítica de las organizaciones pro derechos humanos, que consideraban estas técnicas de vigilancia indiscriminada a los ciudadanos como excesivamente agresivas y vulneradoras de derechos.

Si bien es cierto que este tipo de tecnologías pueden ser utilizadas para limitar el ejercicio de los derechos fundamentales de los ciudadanos cuando se destinen a prácticas como la censura o la intercepción ilícita de comunicaciones, también pueden utilizarse para fines totalmente opuestos. Las herramientas de análisis y divulgación de datos pueden utilizarse como medio de difusión de información en estados sometidos a regímenes gubernamentales autoritarios, pueden abrir una nueva ventana a la transmisión e intercambio de información y conocimiento en todo el mundo y pueden, por supuesto, ayudar a los estados en la lucha contra el crimen organizado y el terrorismo. Utilizadas de forma adecuada, estas herramientas pueden ser un elemento más para favorecer el respeto de los derechos fundamentales en todo el mundo.

La diferencia entre el uso proporcionado y el intrusivo de este tipo de tecnologías de vigilancia debe estar bien delimitado por los estados y las organizaciones supranacionales como la Unión Europea. Los instrumentos legislativos como la Directiva de Protección de Datos de la UE no son suficientemente específicos para regular algo tan complejo como el uso de las tecnologías de análisis de datos, por lo que es necesario dar un paso más. Las autoridades europeas que controlan el cumplimiento de la ley deben asegurar el respeto y la salvaguarda de los derechos recogidos en la Carta de Derechos Fundamentales de la Unión y, por lo tanto, del derecho a la intimidad y la vida privada. La intrusión en el domicilio de una persona es una violación flagrante de estos derechos, en este contexto, el "domicilio virtual" de una persona también debería protegerse en el mismo contexto. El derecho a la protección de datos personales se une al derecho a la intimidad cuando los datos privados de una persona están siendo procesados. La intromisión del estado y de las fuerzas de seguridad en este tipo de

derechos debe fundarse en una norma con rango de ley, en la que se establezcan los límites y garantías de esa intromisión, en pos de preservar los derechos enunciados.

En este sentido se pronunciaba el Tribunal Europeo de Derechos Humanos en el Asunto *Shimovolos v. Russia* en 2011[28]; "La ley debe ser suficientemente clara para dar a los ciudadanos una idea adecuada de las condiciones y circunstancias en que las autoridades están facultadas para recurrir a medidas de vigilancia y de recolección de datos e información personal de los ciudadanos de forma encubierta". Pero no solo se fundamentarán en la ley este tipo de medidas, sino que deberán ser supervisadas en todo caso por el poder judicial. El TEDH se refería a este necesario control jurisdiccional en la sentencia del *Asunto Rotaru vs. Romania*[29]; "*Para que los sistemas de vigilancia encubierta sean compatibles con el artículo 8 del Convenio, deben respetar los principios enunciados en la ley y deben ser supervisados por los organismos e instituciones competentes. Los procesos de supervisión y control deben seguir estrictamente los principios democráticos, reforzando el estado de derecho, como expresamente recoge el Preámbulo del Convenio. El Estado de Derecho trae consigo, entre otras cosas, la necesidad de que cualquier práctica limitativa de los derechos de los ciudadanos esté sometida al control del poder judicial, pues este control entraña la garantía de independencia, imparcialidad y proporcionalidad"*.

La ley y la jurisprudencia españolas se pronuncian en el mismo sentido cuando estamos ante la toma de medidas de vigilancia restrictivas de derechos fundamentales. Sin embargo, este control judicial tampoco se impone como absoluto, en cualquier caso. Existen varias sentencias del Tribunal Constitucional Español (TC, en adelante) que justifican la necesidad de tomar este tipo de medidas sin autorización expresa del poder judicial, pero solo en casos tasados y de especial urgencia. En este sentido se pronunció el TC en la conocida Sentencia 173/2011 de 7 de noviembre[30] que declaró

[28] ***Shimovolos vs. Russia***, 30194/09, TEDH, 21 de junio de 2011: *"The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law."*

[29] ***Rotaru vs. Romania***, 28341/95, TEDH, 4 de mayo de 2000

[30] ***Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre de 2011***. Recurso de amparo 5928-2009

constitucionalmente justificado el acceso a los archivos de un portátil por parte de la Policía sin el consentimiento de su dueño y sin contar con una orden judicial al efecto. En este asunto, un informático a quien se le había encomendado la reparación de un ordenador personal, encontraba durante la reparación varias carpetas con imágenes pornográficas de adolescentes pertenecientes al propietario del ordenador. El informático entregó el mismo a la policía que, sin obtener la previa autorización judicial, accedió a los archivos. El dueño del ordenador fue finalmente condenado como autor de un delito de distribución de material pornográfico infantil. Para justificar la procedencia de la medida tomada por la policía, el TC hacía referencia a la urgencia y necesidad de la intervención policial de los documentos y archivos informáticos del investigado, a fin de determinar si había o no conducta delictiva : *«la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad»* Cuando la gravedad de la conducta, la urgencia y la necesidad justifiquen la intervención de la autoridad en un determinado asunto, se podrá proceder sin la supervisión del poder judicial, que, sin embargo, deberá obtenerse a posteriori con la mayor brevedad posible.

5. Uso de drones

Los comúnmente llamados “drones”, son los vehículos aéreos no tripulados - *UAV (Unmanned Aerial Vehicle)* en inglés – es decir, aeronaves que vuelan sin tripulación. Esta tecnología puntera ha llegado hace poco al uso civil, pero lleva años siendo utilizada en aplicaciones militares, como vehículo de inspección, vigilancia e incluso ataque. Los drones son capaces de mantener de manera autónoma el vuelo, el cual puede ser controlado remotamente o previamente establecido en un plan de vuelo pre programado.

La principal controversia de este tipo de tecnología autónoma que no necesita del ser humano para realizar sus funciones, es precisamente la posibilidad de que estos artilugios no tripulados puedan causar daños colaterales a objetivos erróneamente identificados. Es por ello que su aplicación militar es tan controvertida, aunque también se utilicen en labores más pacíficas como la lucha contra incendios, la supervisión de oleoductos y la seguridad civil.

Este tipo de vehículos aéreos no pilotados surgieron en la década de los 70 y fueron desarrollados por las Fuerzas Aéreas de Israel. Su uso comenzó a implantarse a partir de los años 90 en el ámbito militar, como herramienta principal en las misiones de reconocimiento. Tras los ataques terroristas de Nueva York y Washington del 11 de septiembre de 2001, los Estados Unidos comenzaron a utilizar los primeros drones armados en Yemen en 2002, transformando el propósito inicial de vigilancia y control con que habían sido ideados estos elementos, para convertirlos en máquinas capaces de realizar ataques en zonas remotas, con solo pulsar un botón. Los drones incorporan en su sistema un conjunto de cámaras de alta resolución e infrarrojos, capaces de transmitir imágenes en tiempo real y de captar e identificar un objetivo en tierra desde el aire.

Tradicionalmente concebidos como un medio para realizar acciones de vigilancia en zonas de conflicto, también han sido utilizadas para permitir el acceso a zonas aisladas, afectadas por desastres naturales, ataques químicos o biológicos…

Desde su creación, el uso de drones se ha generalizado. Los drones actuales no solo son capaces de mantener el vuelo durante más tiempo y a mayor distancia del centro de control, sino que han incorporado también sistemas de aterrizaje automático e incluso están siendo programados para ser capaces de tomar decisiones autónomas en momentos críticos. Este hecho ha traído consigo situaciones como la muerte de cientos

de civiles, entre ellos niños, causadas por el error de estas máquinas en la detección de objetivos en las zonas de conflicto. Ante estas circunstancias, se plantea un debate ético y moral sobre el uso de drones armados autónomos en estas zonas en guerra.

Naciones Unidas lleva años pidiendo a la comunidad internacional que cese en el uso de este tipo de vehículos aéreos armados hasta que exista una mayor base legal para su uso y, en todo caso, que respeten las leyes internacionales existentes y permitan que se lleven a cabo las investigaciones precisas en los casos en que se hayan reportado ataques ilícitos sobre población civil.

El uso de estos vehículos no tripulados se ha extendido tanto en los últimos años que su uso hoy en día es generalizado, tanto en su aplicación militar y de seguridad nacional, como en el uso privado particular. En sus nuevas versiones los drones no son solamente armas militares, sino que se utilizan para fines más nobles y que innegablemente interfieren menos con los derechos humanos. Hoy en día los drones se utilizan en operaciones de rescate y salvamento, en eventos deportivos o grandes aglomeraciones de personas, para la vigilancia del tráfico o la exploración de territorios salvajes y el estudio de sus especies vegetales y animales. Son capaces de transmitir, no solo imágenes, sino datos meteorológicos, niveles de radiación o de concentración de gas etc., y todo a tiempo real. Capaces de llegar a zonas no accesibles para el hombre o para otro tipo de vehículo tripulado, sus aplicaciones positivas son infinititas y suponen un menor coste moral y ético.

Los rápidos avances tecnológicos y la alta capacidad de monitorizar objetivos y transmitir datos en tiempo real, han llamado la atención de los gobiernos nacionales y supranacionales que buscan una aplicación de los drones más encaminada a la vigilancia, seguridad y prevención del terrorismo, que a un uso militar. Su aplicación en las medidas de seguridad nacional ha sido valorada positivamente por los organismos de control del respeto a los derechos fundamentales, siempre que se destine al control de "áreas donde la expectativa individual de privacidad no esté bien definida". La Unión Americana de Libertades Civiles se opone a la realización rutinaria de sesiones de vigilancia aérea sobre población civil, pues entiende que otorga un poder demasiado extenso al Estado que estaría capacitado para monitorizar, seguir y grabar a cualquier individuo en su día a día, convirtiéndose en un espía de sus propios ciudadanos.

El problema del uso de drones no viene dado únicamente por su uso gubernamental; cada vez hay más y más personas que utilizan este tipo de vehículos de modo particular, ya sea para el ejercicio de su profesión como para el uso recreativo. Aunque a día de hoy no existe propiamente un marco regulatorio claro en el ámbito de la UE - especialmente en lo referente a los drones de uso particular y de menos de 150kg, que no entrarían dentro de lo que la Agencia Europea de Seguridad Aérea (en adelante, EASA) considera un UAV (Unmanned Aerial Vehicle) y que sí están regulados en el *Reglamento 216/2008 de Normas Comunes en el Campo de la Aviación Civil*[31]– el uso de drones por particulares sí está regulado en varios estados pertenecientes a la UE, como República Checa, Dinamarca, Suecia, Alemania, Reino Unido o España. El fin que persigue la UE es precisamente seguir el ejemplo de estos estados miembros para crear una norma europea que unifique el uso de drones – independientemente de su tamaño o peso - en toda la Unión. Precisamente ha sido en este último año 2016 en el que la EASA ha presentado una primera propuesta regulatoria a la Comisión[32], después de que el año pasado elaborara una Opinión Técnica[33], en la que clasificaba los drones en tres niveles de riesgo - bajo, medio y alto – según las características del vehículo y el uso que pretendía hacerse de él. En este texto, la EASA reflexiona sobre la importancia de crear una norma que, junto con las leyes nacionales, garantice el uso responsable de los UAV, el respeto a la privacidad, la protección de datos y el medio ambiente. Así, en este proyecto legislativo se enumeraban algunos de los requisitos que deberán respetarse en manejo de drones;

- Los pilotos de drones de alta gama, especialmente aquellos que superen los 150 kg de peso, deberán registrarse formalmente para obtener una licencia que les permita manejarlos
- Los Estados Miembros podrán limitar e incluso prohibir el vuelo de estos aparatos en determinadas zonas, por razones de seguridad o especial peligrosidad.

[31] ***REGLAMENTO (CE) No 216/2008*** DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de febrero de 2008 sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia Europea de Seguridad Aérea, y se deroga la Directiva 91/670/CEE del Consejo, el Reglamento (CE) no 1592/2002 y la Directiva 2004/36/CE

[32] Agencia Europea de Seguridad Aérea, ***'Prototype' Commission Regulation on Unmanned Aircraft Operations***, 22 de agosto 2016.

[33]Agencia Europea de Seguridad Aérea, "***Opinion of a technical nature. Introduction of a regulatory framework for the operation of unmanned aircraft",*** 18 de diciembre de 2015

- Los drones no deberán volar cerca de donde operen los servicios de emergencia; hospitales, parques de bomberos, comisarías de policía…
- Deberán cumplirse los requisitos de seguridad mínimos establecidos y otras exigencias técnicas e incluso podrá exigirse al propietario la contrata de un seguro de responsabilidad civil.

Mientras se espera que este proyecto legislativo vea la luz a principios de 2017, en derecho interno también vamos a cerrar 2016 sin la prometida reforma del *Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia*[34]. Este es el primer texto nacional en el que se recogen las normas aplicables a los drones de menos de 150kg de uso particular profesional, - ya que el uso de drones con fines recreativos no tiene todavía una regulación específica - como se contempla en la exposición de motivos; *"Esta Ley establece las condiciones de explotación de estas aeronaves para la realización de trabajos técnicos o científicos o, en los términos de la normativa de la Unión Europea, operaciones especializadas, así como para vuelos de prueba de producción y de mantenimiento, de demostración, para programas de investigación sobre la viabilidad de realizar determinada actividad con aeronaves civiles pilotadas por control remoto, de desarrollo de nuevos productos o para demostrar la seguridad de las operaciones específicas de trabajos técnicos o científicos, permitiendo, de esta forma, su inmediata aplicación."* En este texto se permite únicamente su uso profesional en los siguientes casos;

- 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 aéreos;
- Observación y vigilancia aérea incluyendo filmación y actividades de vigilancia de incendios forestales; publicidad aérea, emisiones de radio y TV,
- Operaciones de emergencia, búsqueda y salvamento

[34] *Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.*

Pues bien, aunque el Gobierno preveía la entrada en vigor de una nueva ley que regulara el uso de drones en España, la compleja situación política que se ha vivido durante el último año ha hecho imposible su creación. Tendremos que esperar un poco más para tener una ley nacional de contenido más amplio previsiblemente hasta mediados del próximo año.

Ahora que conocemos la escasa y todavía poco clara legislación sobre drones, es el momento de analizar los derechos fundamentales que se ponen en juego con el uso de estos vehículos aéreos. Para ello nos remitimos al estudio realizado por el Comité de Libertades Civiles, Justicia y Asuntos de Interior (*Committee on Civil Liberties, Justice and Home Affairs* o LIBE, en inglés) del Parlamento Europeo, sobre las consecuencias del uso civil de drones en los derechos a la vida privada y la protección de datos[35]. Para elaborar este proyecto, el LIBE se sirvió principalmente de las opiniones del Grupo sobre Protección de Datos del Artículo 29[36] y la opinión del Supervisor Europeo de Protección de Datos[37]. En este informe se reflexiona en torno a la posibilidad de que el uso civil de drones provoque una interferencia grave en la vida privada de los ciudadanos. Los drones, por pequeños que sean, suelen estar equipados de cámaras de video o fotografía que permiten; bien guiar al piloto durante el vuelo, bien captar y almacenar en su interior las imágenes captadas en el aire para su posterior visualización. Como consecuencia, la vida privada, la propia imagen y los bienes personales quedan expuestos frente a estos drones.

Por otro lado, los drones destinados a la vigilancia, tanto pública como privada, también podrían almacenar y procesar datos e imágenes de gran cantidad de población, pudiendo interferir e incluso violar los derechos anteriormente enunciados de estas personas, que

[35] Directorate General for Internal Policies: Civil liberties, justice and home affairs of the European Parliament ***Privacy and Data Protection Implications of the Civil Use of Drones*****,** Brussels June 2015

[36] ***El Grupo sobre Protección de Datos del Artículo 29*** o "*Article 29 Data Protection Working Party" fue creado por la Directiva 46/95 de Protección de Datos del Parlamento y el Consejo, el 24 de octubre de 1995. Es un órgano de carácter consultivo y que actúa de forma independiente. Se compone de:*

- Un representante de la autoridad nacional, designado por cada Estado Miembro
- Un representante designado por las instituciones de la UE
- Un representante elegido por la Comisión Europea

[37] ***Opinión del Supervisor Europeo para la Protección de Datos*** con respecto a la Comunicación de la Comisión al Parlamento y al Consejo llamada *"La nueva era de la aviación. La apertura del mercado de la aviación al uso particular y civil de vehículos aéreos no pilotados, de forma sostenible"*, 26 de noviembre de 2014

estarían sometidas a una vigilancia continuada sin saberlo y sin ser conscientes de ello. En opinión del Supervisor Europeo de Protección de Datos, el problema no es lo que estos aparatos son capaces de captar durante su vuelo, sino el uso que posteriormente se dé a esa información. El material obtenido por las cámaras integradas en los drones es susceptible de utilizarse en fines comerciales, profesionales, privados e incluso en investigaciones policiales o de los servicios de inteligencia gubernamentales. No es posible, por lo tanto, que no exista formalmente una normativa que limite en cierto modo el uso de estos aparatos o que se pronuncie al menos sobre las responsabilidades en que pueden incurrir quienes hagan un uso indebido de las imágenes captadas por los mismos.

El LIBE llegaba a las siguientes conclusiones:

- La captación de imágenes de los drones de uso privado interfiere con lo establecido en el Artículo 8 del Convenio Europeo de Derechos Humanos y el Artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, pues desafían los derechos de privacidad garantizados a los ciudadanos de la UE y esta interferencia solamente es válida y proporcional en determinadas situaciones contempladas en la ley y bajo ciertas condiciones y salvaguardas.
- El uso privado de drones cae dentro del alcance de la Directiva 46/95 de protección de datos de carácter personal y deberá respetar sus prerrogativas. Así mismo, los datos procesados posteriormente para fines comerciales deberán cumplir escrupulosamente con las normas de transposición nacionales de la Directiva de Datos 46/95.
- La publicación de las imágenes obtenidas en Internet o en medios de comunicación, sin ningún fin informativo específico, no entrará dentro de lo establecido en el *Artículo 9. "Tratamiento de datos y libertad de expresión"*[38] de la Directiva 46/95

[38] ***Directiva 46/95 de Protección de Datos de Carácter Personal***. *Artículo 9. Tratamiento de datos personales y libertad de expresión*: "En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, 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."

- El uso de drones y el proceso de las imágenes obtenidas mediante su uso, por parte de las autoridades de un Estado Miembro, de las agencias de inteligencia o de cualquier otro organismo gubernamental o supranacional deberá respetar las leyes relativas a los derechos de privacidad y protección de datos. Solo se considerará un uso justificado cuando persigan un fin legítimo, necesario en un estado democrático y la medida de seguimiento tomada pueda considerarse proporcionada al propósito perseguido.

Para el LIBE era muy importante recomendar a las instituciones la creación de un marco normativo más concreto en torno al uso civil de drones. Solo de esta forma se podría transmitir a los usuarios información suficiente para que estos conocieran el potencial intrusismo de estas tecnologías en los derechos fundamentales de vida privada y protección de datos de los ciudadanos. Asimismo, en el marco de la vigilancia por parte de las autoridades nacionales, se recomendaba a estas el cumplimiento de las normas de protección de los derechos fundamentales y un respeto escrupuloso a los principios de necesidad, proporcionalidad, idoneidad en la toma de medidas vulneradoras de estos derechos. Y recuerda que estas medidas deberán estar siempre fundadas en la ley y sujetas al control jurisdiccional.

IV. CONCLUSIÓN. LOS SERVICIOS DE INTELIGENCIA DE LOS ESTADOS MIEMBROS DE LA UE Y LAS GARANTÍAS DE RESPETO A LOS DERECHOS FUNDAMENTALES.

Las tecnologías de detección de personas y de seguridad nacional que hemos analizado en este trabajo son gestionadas, en su mayor parte, por las autoridades nacionales de cada uno de los Estados Miembros; ejército, policía y Ministerio del Interior principalmente. De este modo, las leyes que recogen este tipo de medidas restrictivas de derechos fundamentales no siempre son iguales. Partiendo del principio de supremacía del derecho comunitario, sería lógico pensar que las legislaciones de los veintiocho respetan por igual los principios contenidos en la Carta de los Derechos Fundamentales y en el Convenio Europeo de los Derechos Humanos, al que están ligados todos los Estados Miembros.

Para garantizar esto, el Tribunal Europeo de los Derechos Humanos ha promovido en varios de sus pronunciamientos un concepto llamado *"quality of the law"* o *"calidad legislativa"*, que trata de asegurar que los Estados Miembros elaboren normas que regulen los sistemas de vigilancia, inteligencia y seguridad nacional de forma suficientemente extensa y detallada. Como exponía el Comisario de Derechos Humanos del Consejo de Europa en su artículo titulado "El Control Efectivo de los Sistemas de Seguridad Nacionales"[39]*; "Los sistemas de seguridad nacional y los servicios de inteligencia son, por sus características y prerrogativas, susceptibles de llevar a cabo acciones vulneradoras de derechos fundamentales cuando se realicen sin el suficiente control y sujeción a una ley efectiva. Están dotados de poderes muy invasivos que pueden ser utilizados de manera discrecional, de forma encubierta y, en algunos países, pueden ser considerados como instrumentos del gobierno utilizados con fines políticos".* Siendo de este modo, la creación de una ley exhaustiva que dé cobertura a estos sistemas de vigilancia es imperativa; tanto en el ámbito nacional como supranacional.

La ley que contemple estas medidas intrusivas deberá ser accesible para los ciudadanos que vean restringidos sus derechos, aunque esto no es un principio absoluto, ya que como indicaba el TEDH en la sentencia del Asunto W y S vs. Alemania[40]; *"Las normas reguladoras de medidas secretas de vigilancia y control de los ciudadanos - como la intercepción de las comunicaciones – no pueden ser tan previsibles como para permitir al ciudadano medio averiguar cuando las autoridades van a proceder a interceptar sus comunicaciones, de modo que este pueda modificar su comportamiento en respuesta (…) Sin embargo, el riesgo de arbitrariedad de los poderes públicos en la toma de estas medidas es evidente, especialmente cuando se toman de forma encubierta. (…) Por ello es esencial tener leyes detalladas y claras que establezcan las circunstancias y condiciones en que las autoridades están legitimadas para tomar semejantes medidas de control".*

Por lo tanto, la sujeción a la ley debe ser exhaustiva pero no absoluta. El TEDH establecía otro concepto de gran importancia ligado al "*quality of the law*"; las garantías mínimas o *"minimun safeguards"* que deben establecerse en las leyes de

[39] Comisario de Derechos Humanos del Consejo de Europa***, "Democratic and effective oversight of national security services***", mayo de 2015

[40] ***Weber and Saravia vs. Germany,*** *Nº 54934/00, TEDH, 29 de junio de 2006*

funcionamiento de los servicios de vigilancia y seguridad nacional para evitar los abusos de poder[41].

La seguridad nacional, en sentido estricto, implica la protección de la población civil frente a las amenazas y los daños físicos efectivos que puedan sufrir. Mediante el contrato social. Los Estados se comprometen a garantizar esta seguridad, a cambio del poder de coartar o limitar las libertades de los ciudadanos. En los Estados democráticos, los ciudadanos y el Estado aceptan este compromiso, estableciendo unos principios básicos que no pueden ser ignorados por ninguna de las partes del contrato social; la salvaguarda de la dignidad, la libertad y la justicia, así como el respeto a los Derechos Fundamentales. Todos los Estados que conforman la Unión Europea comparten estos y otros principios de igual relevancia; educación, sanidad, igualdad, democracia… Todo esto no puede ignorarse en el ámbito de la seguridad nacional.

La salvaguarda de estos principios fundamentales de la UE nos obliga a conseguir un sistema en el que las tecnologías de vigilancia y control de personas en el ámbito de la seguridad nacional se apliquen de forma proporcional y efectiva, siempre garantizando la menor injerencia a los derechos fundamentales, que son el culmen de lo que hemos conseguido como sociedad democrática en el último siglo.

Así como se reconoce la legitimidad de los Estados Miembros para establecer los medios de control ya referidos, se reconoce que cualquier intrusión de los poderes públicos en la esfera de los derechos fundamentales debe estar justificada en la ley y sujeta al control jurisdiccional. Debe respetar la dignidad humana y ser proporcional y necesaria.

Los valores comunes que los veintiocho Estados Miembros de la UE plasmaron en la Carta de los Derechos Fundamentales deben ser el marco normativo a partir del cual se construya un concepto de seguridad nacional más respetuoso con esos derechos.

[41] *"* In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law to avoid abuses of power: *the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."* ***Asunto Weber and Saravia vs. Germany,*** *Nº 54934/00, TEDH, 29 de junio de 2006, p. 95.*

Además, debe maximizarse el respeto y la cooperación de los veintiocho estados, como garantía de la confianza existente entre todos ellos, como miembros de una sola Unión Europea.

Madrid, a 15 de enero de 2017

BIBLIOGRAFÍA

1. Libros, trabajos monográficos, artículos y obras colectivas

- ROBERT ALEXY, *Teoría de los Derechos Fundamentales*, Centro de Estudios Constitucionales, Madrid, 1993.

- ANTONIO MAGDALENO ALEGRÍA, "Libertad de expresión, terrorismo y límites de los Derechos Fundamentales", *Revista de Derecho Político de la Universidad Nacional de Educación a Distancia* (UNED) Vol. 69, 2007

- MARÍA JOSÉ CABEZUDO BAJO "La restricción de los Derechos Fundamentales: un concepto en evolución y su fundamento constitucional" *Revista de Derecho Político de la Universidad Nacional de Educación a Distancia* (UNED) Vol. 77, 2010.

- UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO), "Global survey on Internet Privacy and Freedom of Expression. Series on internet freedom", 2012

- PIET HEIN VAN KEMPEN, "Four concepts of security: a human rights perspective", *Human Rights Law Review*, Vol. 13, March 2013.

- COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, "Una nueva era de la aviación: Abrir el mercado de la aviación al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible", Comisión Europea, abril de 2014.

- THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, "Ethics of Security and Surveillance Technologies", European Commission, May 2014

- EUROPEAN PARLIAMENT RESEARCH SERVICE, "Mass surveillance, Part 2: Technology foresight", January 2015

- MICHELLE CAYFORD, COEN VAN GULIJK (TU DELFT), ERIK KREMPEL (FRAUNHOFER), JUHA LAVAPURO, TUOMAS OJANEN, MARTIN SCHEININ (EUI), JOHN GUELKE, HELEN MCCABE, TOM SORELL (UW) AND SEBASTIAN SPERBER (EFUS), "SURVEILLE. Surveillance: Ethical issues, legal limitations, and efficiency", *Seventh Framework Programme,* (FP7 SEC 2011 284725), April 2015

- THE INFORMATION COMMISSIONER'S OFFICE (ICO) OF THE UK, "In the picture: A data protection code of practice for surveillance cameras and personal information", May 2015

- DIRECTORATE GENERAL FOR INTERNAL POLICIES: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, "Privacy and Data Protection Implications of the Civil Use of Drones", European Parliament, June 2015

- THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), "Dissemination and use of intrusive surveillance technologies", December 2015

- AGENCIA EUROPEA DE SEGURIDAD AÉREA, "Opinion of a technical nature. Introduction of a regulatory framework for the operation of unmanned aircraft", December 2015

- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, "Surveillance by intelligence services: fundamental rights safeguard and remedies in the EU. Mapping Member States' legal frameworks", 2016.

- AGENCIA EUROPEA DE SEGURIDAD AÉREA, "Prototype' Commission Regulation on Unmanned Aircraft Operations", August 2016.

2. Documentos oficiales e institucionales

- *CONVENIO EUROPEO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y LAS LIBERTADES FUNDAMENTALES*, y Protocolo Adicional nº 1; Convenio de Roma de 1950, Consejo de Europa

- R. Alonso García, *Tratado de Lisboa y versiones consolidadas de los Tratados de la Unión Europea y de Funcionamiento de la Unión Europea*, Editorial: Civitas, 4ª Edición de 2013, Colección: Serie Menor

- *CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA*, nº 2000/C 364/01, ratificada el 7 de diciembre de 2000 por el Parlamento Europeo, Consejo Europeo y Comisión Europea

- CONSTITUCIÓN ESPAÑOLA DE 1978, Boletín Oficial del Estado núm. 311, de 29 de diciembre de 1978, páginas 29313 a 29424

- 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. Artículo 2. a) y b)

- REGLAMENTO DE EJECUCIÓN (UE) 2015/187 DE LA COMISIÓN de 6 de febrero de 2015 por el que se modifica el Reglamento (UE) no 185/2010 en lo que se refiere a la inspección del equipaje de mano

- REGLAMENTO (UE) 2016/1710 DEL CONSEJO de 27 de septiembre de 2016 por el que se modifica el Reglamento (CE) no 2580/2001 sobre medidas restrictivas específicas dirigidas a determinadas personas y entidades con el fin de luchar contra el terrorismo

- REGLAMENTO (CE) No 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de febrero de 2008 sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia Europea de

Seguridad Aérea, y se deroga la Directiva 91/670/CEE del Consejo, el Reglamento (CE) no 1592/2002 y la Directiva 2004/36/CE

3. Jurisprudencia

A. Jurisprudencia del Tribunal Europeo de los Derechos Humanos

- Sentencia del Tribunal Europeo de Derechos Humanos (en adelante, TEDH), 4 de diciembre de 2008, *asunto S. & Marper v. United Kingdom* nº 30562/04 -30566/04

- Sentencia TEDH, 25 septiembre de 2001, *asunto P.G. y J.H. vs. Reino Unido.* nº 44787/98

- Sentencia TEDH, enero de 2003, *asunto Peck vs. Reino Unido*, nº 44647/98

- Sentencia TEDH, 31 de mayo de 2005, *asunto Vetter vs. France*, nº 59842/00

- Sentencia TEDH, 21 de junio de 2011, *asunto Shimovolos vs. Russia*, nº 30194/09

- Sentencia TEDH, 4 de mayo de 2000, *asunto Rotaru vs. Romania*, nº 28341/95

- Sentencia TEDH, 27 de mayo de 2014, *asunto De la Flor Cabrera vs. Reino de España*, nº 10764/09

- Sentencia TEDH, 2 de diciembre de 2010, *asunto Uzun v. Germany*, nº 35623/05

B. Jurisprudencia del Tribunal de Justicia de la Unión Europea

- Sentencia del Tribunal de Justicia de 13 de abril de 2000, *asunto Kjell Karlsson y otros. Petición de decisión prejudicial: Regeringsrätten – Suecia*, C-292/97

- Sentencia del Tribunal de Justicia de la Unión Europea de 29 de enero de 2008, *asunto Productores de España vs. Telefónica de España SA*, C-275/06, FJ 63.

- Sentencia del Tribunal de Justicia de la Unión Europea de 11 de diciembre de 2014, *asunto František Ryneš / Úřad pro ochranu osobních údajů*, C-212/2013

C. Jurisprudencia del Tribunal Constitucional y el Tribunal Supremo

- Sentencia del Tribunal Constitucional núm. 173/2011 de 7 de noviembre de 2011. Recurso de amparo 5928-2009

- Sentencia de la Sala de lo Social del Tribunal Supremo núm. 1685/2013 de 13 de mayo de 2014

- Sentencia del Pleno del Tribunal Constitucional núm. 39/2016, de 3 de marzo de 2016. Recurso de amparo 7222-2013.

- Sentencia de la Sala de lo Civil del Tribunal Supremo núm. 678/2014 de 20 de noviembre de 2014.

- Sentencia de la Sala de lo Penal del Tribunal Supremo Núm. 45/2014 de 7 de febrero de 2014