Revista de Derecho Civil
http://nreg.es/ojs/index.php/RDC
ISSN 2341-2216
vol. IX, núm. 4 (octubre-diciembre, 2022)
Ensayos, pp. 351-375

A VUELTAS CON LA PONDERACIÓN DE DERECHOS EN MATERIA DE VIDEOVIGILANCIA

Interés legítimo, seguridad privada, régimen vecinal y protección de datos[1]

Mónica Martínez López-Sáez

Profesora Ayudante Doctora en Derecho Constitucional

Universi*dad* de Valencia

TITLE: *The Balancing of Rights in Video Surveillance Matters: Legitimate Interest, Private Security, Property Regime and Data Protection.*

RESUMEN: El régimen vecinal requiere de una convivencia de personas, y, por tanto, de derechos fundamentales e intereses particulares y generales, en ocasiones, contrapuestos. Entre las potenciales intromisiones a los derechos personalísimos se encuentra precisamente la relativa al tratamiento de datos de carácter personal mediante sistemas de videovigilancia, instalados con fines de garantizar la seguridad de las instalaciones, los bienes y las personas. Para los casos en los que media un acuerdo válido de Junta de Propietarios y consta la oposición de un comunero alegando la vulneración de su derecho a la intimidad, a la vida privada y familiar y a la protección de datos, ahora contamos con la postura del TJUE, que se ha pronunciado, por primera vez, sobre esta cuestión. La presente contribución analiza la STJUE 11 de diciembre de 2019 (relativa al asunto C-708/18, TK y Asociaţia de Proprietari bloc M5A-ScaraA) y perfila algunas cuestiones relativas al test de ponderación establecido para lidiar con el binomio interés legítimo en el tratamiento/protección de datos de carácter personal.

ABSTRACT: The property regime requires the coexistence of individuals and, therefore, of often-time conflicting fundamental rights and particular and general interests alike. Among the potential interferences on personality rights we must include those relating to the processing of personal data by means of video surveillance systems, installed for the purpose of guaranteeing the security of property and the safety and health of persons. For those cases in which there is a valid building general assembly agreement and the opposition of one of the co-owners alleging the infringement of their right to privacy, to private and family life and to data protection, we now have the position of the CJEU, which has ruled for the first time on this issue. The present contribution analyzes judgment 11 December 2019 (concerning case C-708/18, TK and Asociaţia de Proprietari bloc M5A-ScaraA) and outlines some questions concerning the balancing test established to deal with the binomial legitimate interest in the processing-protection of personal data.

PALABRAS CLAVE: Videovigilancia, protección de datos, seguridad privada, uso residencial, interés legítimo, test de ponderación

KEY WORDS: Videosurveillance, data protection, private security, residential use, legitimate interest, balancing test.

[1] Este trabajo se ha realizado en el marco del Proyecto de Investigación RTI2018-095367-B-I00 (Ministerio de Ciencia, Innovación y Universidades, IP Rosario García Mahamut y Cristina Pauner Chulvi), relativo a la implementación del RGPD en España y el análisis de la LOPDGDD.

1. ASPECTOS INTRODUCTORIOS Y PUNTOS DE PARTIDA EN CLAVE CIBERNÉTICA Y JURÍDICA

En aras de la claridad (conceptual), vemos importante explicar nuestra decisión de hablar de la seguridad privada, expresión que hemos utilizado como sinónimo de seguridad en el ámbito de la vida privada y familiar (en el marco de una comunidad de vecinos/aplicable a los regímenes de propiedad horizontal) a la vez que como concepto material de la Ley 5/2014, de 4 de abril, de Seguridad Privada[2].

1.1. *El derecho a la protección de datos como respuesta ante los retos de las NTIC*

La tecnociencia sigue avanzando de una manera sin precedentes, afectando a todas las facetas de la vida cotidiana. Las Nuevas Tecnologías de la Información y la Comunicación (en adelante «NTIC»), en sí mismas, y el uso que se hace de ellas, han difuminado las fronteras físicas y temporales, lo que posibilita, agiliza y diversifica relaciones de toda índole (comerciales, financieras, políticas, culturales, personales, etc.)[3]. Y es en este nuevo panorama que ha surgido la necesidad de regular estos nuevos fenómenos del progreso tecnológico y socio-económico, y proteger de manera efectiva los derechos más fundamentales de las personas.

La era actual se ha venido llamando, en los últimos años, la era del «capitalismo de vigilancia»[4]. Ante desafíos globales, sobre todo los que comprometen y erosionan

[2] Los servicios de videovigilancia incluidos en dicha ley son los que sirven para prevenir y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, incluida aquella videovigilancia relativa a la utilización de cámaras cuyo objeto principal es la comprobación del estado de instalaciones y el control de accesos (la habitual de las comunidades de propietarios).

[3] Hay sectores enteros de la vida cotidiana, allende de la propia economía, que dependen, en su práctica totalidad, de datos de carácter personal para funcionar de manera efectiva, requiriendo y favoreciendo el almacenamiento, procesamiento y transmisión masiva de información personal. Las NTIC y los datos personales se han convertido en las fuerzas motoras y habilitadoras y presenciamos, en definitiva, una auténtica alteración de la forma en la que interactúan las personas, el aparato estatal y el privado, entre ellos y entre sí, precisamente debido a la escala acelerada y modo radical en el que se intercambian y se utilizan la información personal.

[4] Zuboff, S., *The Age of Surveillance Capitalism,* London, Profile Books Ltd, 2019. Basada en la recogida, almacenamiento, análisis, utilización e intercambio masivo e ilimitado de información de carácter

gravemente los derechos, y por ende, inciden en valores como la libertad, la igualdad y la dignidad, el Derecho, desde todas sus ópticas y disciplinas, debe también responder en sentido global; sin poner freno al progreso en sí mismo, sí debe delimitarlo a través de su reglamentación jurídica, y reforzar el estatuto jurídico de la persona, instaurando mecanismos de garantía para el efectivo disfrute de sus derechos. Cuando hablamos de los derechos humanos y su relación con las NTIC, vemos que el Derecho despliega todo su arsenal y vemos cómo ejecuta sus diferentes funciones[5]. Dada esta mutación informática y digital que supone las últimas generaciones de las NTIC, hace necesaria una revisión de su papel en la sociedad, su relación con el Derecho y las delimitaciones que les serán aplicables en aras de evitar injerencias desproporcionadas a los derechos y libertades de las personas. Como se ha expuesto en otro lugar, el carácter fundamental del derecho a la protección de datos experimentó una consagración sincrónica en instancias nacionales y europeas[6].

El actual marco europeo de protección de datos se compone, principalmente, del Reglamento General de Protección de Datos («RGPD», en adelante)[7] que entró en

personal ya no sólo por parte de organismos al servicio del Estado sino también (y sobre todo) por parte de entidades con fines privados.

[5] Su función reguladora es la más evidente. El Derecho, como herramienta para mantener el orden, resolver conflictos y proteger los derechos y libertades de los ciudadanos, debe establecer normas que ponderen los intereses en juego. La reglamentación jurídica de la informática ha revestido un interés significativo, además de prioritario, debido a que la respuesta jurídica tiende a ir muy por detrás de los problemas tecnológicos: una suerte de juego cruel entre el inalcanzable correcaminos tecnológico y el coyote jurídico. El Derecho suele parchear los baches y los agujeros que la Tecnología genera en el aparato social y jurídico. Con independencia de cuál sea la nomenclatura de preferencia, el Derecho Informático (o nociones afines como Derecho Telemático, Tecnológico, De la Sociedad de la Información, De Internet, Del Ciberespacio, de las NTIC, entre otras muchas) pretende dar respuesta a los retos y desafíos jurídicos provocados por las NTIC y el uso que se hace de ellas.

[6] De ahí nace el derecho a la protección de datos como nuevo derecho o derecho emergente. No hay lugar a duda de que el sistema europeo de protección de datos es tanto un sistema de atribución de derechos como un sistema cuyo diseño e interpretación son consistentes con la concepción subyacente de un derecho fundamental, el de la protección de datos, que es, a su vez, instrumento para proteger otros derechos personalísimos íntimamente ligados al mismo (derecho a la intimidad, derecho a la vida privada y familiar, derecho al honor y a la imagen, etc.). La consagración sincrónica a la que se hace referencia ha ocurrido en instancias nacionales (con su materialización legislativa *ad hoc* o constitucional-como fue el caso español-) y europeas, con directrices y convenios regionales y con la adopción de la Carta de Derechos Fundamentales de la UE («CDFUE», en adelante) en 2000 (y su posterior consagración como instrumento jurídico vinculante con el mismo valor que los tratados constitutivos y como piedra angular de las fuentes del sistema de protección de los derechos fundamentales de la UE como reza el art. 6 TUE tras la reforma de 2007). *Vid*. Martínez López-Sáez, M., «Hacia una integración digital europea: la constitucionalización del derecho de la UE y la europeización del Derecho Constitucional en materia de protección de datos», *Revista de Estudios Europeos*, *71*, 2017, pp. 23-37; y más recientemente, Martínez López-Sáez, M., «Repensando el Derecho Constitucional a la Protección de Datos ante la Mutación de la Informática», En J. Martín Cubas (Ed.), *Repensando la Constitución 40 años después*, Valencia, Tirant Lo Blanch, 2019, pp. 147-160

[7] Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

vigor en mayo de 2018, deroga y sustituye a la archiconocida Directiva 95/46/CE («DPD», en adelante)[8]. Aunque en el presente trabajo trataremos la interpretación, por parte del TJUE, de esta segunda, por ser la normativa aplicable en el momento de la controversia nacional que dio lugar a la activación del procedimiento prejudicial europeo, cabe al menos aludir a la necesidad de la modernización en el aparato jurídico relativo a la protección de datos en la UE. En este sentido, es importante subrayar que la DPD se adoptó en un momento en el que el desarrollo de la innovación tecnológica y la transformación digital (en especial la Red) estaban en una fase embrionaria, mientras que los retos planteados en el entorno digital requerían de normas uniformes y eficaces. Así, se pretendía abordar las insuficiencias de la normativa anterior[9], a través de una revisión global del sistema europeo de protección de datos. Si bien se puede argumentar que el RGPD ha supuesto «un antes y un después»[10], decir que dicho instrumento jurídico cambia radicalmente el marco de protección de los datos de carácter personal en la UE quizás sería una afirmación un tanto simplificada. Pese a ello, se podría decir que el proceso ha concluido con una legislación fortalecida y ambiciosa destinada a transformar la manera en la que se utilizan (y se controlan) los datos de carácter personal en la era tecno-digital actual.

1.2. *El binomio «informática-derechos» en el marco del régimen de propiedad horizontal: singularidades y cuestiones de interés*

El régimen vecinal requiere no sólo una convivencia que implica, en muchas ocasiones, un choque frontal de intereses y bienes constitucionalmente protegidos, lo que, a su vez, genera la necesidad de garantizar la dignidad y la libertad en situaciones poco delimitadas. En palabras del filósofo Jean-Paul Sartre «Mi libertad se termina dónde empieza la de los demás». Esta realidad socio-jurídica sobre el ejercicio y límites a la

circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en:
http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[8] 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. Disponible en:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

[9] *Vid*., por ejemplo, Rallo Lombarte, A., «Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma», *Revista de Derecho Político (UNED), 85*, p. 16; García Mahamut, R., «Del Reglamento General de Protección de Datos a la LO 3/2018 de Protección de Datos Personales y Garantías de los Derechos Digitales» En R. García Mahamut, y B. Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales,* Valencia, Tirant Lo Blanch, 2019, pp. 97-98.

[10] *Vid*., por todos, Murillo De La Cueva, P.L., «El Tribunal Supremo y el derecho a la protección de datos» En R. García Mahamut, y B. Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales.* Valencia: Tirant Lo Blanch, 2019, p. 181.

libertad debe también trasladarse a los reductos más «domésticos»[11], incluidas las relaciones con los vecinos y los gestores de un edificio en régimen de propiedad horizontal.

La protección y conciliación de los «viejos» y «nuevos» derechos[12] de la personalidad (intimidad, vida privada y familiar, honor, y protección de datos, respectivamente, por nombrar algunos) se ve claramente en el caso que nos ocupa: la videovigilancia en el ámbito residencial. La instalación de cámaras de videovigilancia y el tratamiento de los datos personales recabados (principalmente, las imágenes grabadas) presenta especial interés. Sin entrar a examinar el caso de decisiones unilaterales sobre la instalación de sistemas de videovigilancia por parte de un comunero para dar seguridad a su hogar, nos centraremos en el caso de que medie un acuerdo válido de Junta de Propietarios y conste la oposición de un comunero. Dicho lo anterior, procedemos, de manera sucinta, a referenciar las singularidades y premisas de partida sobre temas relacionados con el objeto de estudio.

En primer lugar, cabe recordar que según la normativa aplicable, la comunidad de propietarios, a pesar de no gozar de personalidad jurídica, en tanto colectividad que cuenta con ficheros de datos personales y efectúa un tratamiento de los mismos, se debe considerar como responsable del tratamiento (como persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales), y, por ende, su administrador, se considerará encargado del tratamiento en virtud de su relación contractual con la comunidad (la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento). Esto no sería así en el caso de que una empresa de seguridad fuera la que gestiona el sistema de videovigilancia del edificio, este adquiriría la condición de responsable del tratamiento. En relación con esto, y en segundo lugar, las obligaciones procedimentales genéricas y específicas por parte del responsable y encargado del tratamiento incluyen no sólo aspectos relativos a la obligación de informar a los interesados del tratamiento, sino también aquellos relativos a los principios de seguridad y confidencialidad, y, de manera especial, al

[11] Como ha resumido magistralmente Díaz Martínez: «*la superposición de la propiedad privativa y la existencia de espacios compartidos de común titularidad, en que las relaciones de vecindad imponen sacrificios de los intereses estrictamente individuales […] no es infrecuente reclamar cierto ámbito reservado para el desarrollo dela vida familiar, al amparo de intromisiones ajenas*». *Vid*. Díaz Martínez, A., «Honor. Intimidad y protección de datos personales en las comunidades en régimen de propiedad horizontal», *Derecho privado y Constitución*, *32*, 2018, p. 191.

[12] Rodotà, S., *El derecho a tener derechos.* (trad. Revuelta López, J.). Bolonia, Trotta, 2014, p. 79.

principio de responsabilidad proactiva (una de las novedades más destacables del RGPD)[13].

En tercer lugar, cabe recordar que, en virtud de los principios de limitación de la finalidad y de minimización, se deben recabar solo los datos personales estrictamente necesarios (adecuados, pertinentes y limitados) para finalidades explícitas, determinadas y legítimas; en el caso que nos concierne, serían aquellos fines relativos a la gestión ordinaria de la comunidad. En cuarto y último lugar, cabe también subrayar que, en virtud del principio de licitud, el tratamiento de datos de carácter personal será lícito si este es realizado bajo una de las siguientes bases jurídicas: cuando el interesado ha consentido, cuando es necesario para la ejecución de un contrato o la petición de medidas precontractuales, cuando es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, cuando es necesario para proteger intereses vitales del interesado o un tercero, cuando es necesario para el cumplimiento de una misión realizada en interés público, o cuando es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento (siempre y cuando sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado). Esta última base legitimadora del tratamiento y su correspondiente salvedad ha sido, precisamente objeto de interpretación por parte del TJUE en la sentencia que se estudia a continuación.

2. EL ASUNTO TK Y ASOCIAŢIA DE PROPRIETARI BLOC M5A-SCARAA COMO PUNTO DE PARTIDA EN LA UNIÓN EUROPEA EN RELACIÓN CON EL RÉGIMEN VECINAL E INSTALACIÓN DE SISTEMAS DE VIDEOVIGILANCIA

El asunto *TK y Asociaţia de Proprietari bloc M5A-ScaraA*[14] versaba sobre una controversia relacionada con la presunta vulneración del derecho fundamental a la protección de datos vinculada a la instalación de un sistema de videovigilancia en el marco de una comunidad en régimen de propiedad horizontal. Tras aprobar, en junta general de la comunidad de propietarios, la instalación de cámaras de videovigilancia

[13] Desde una perspectiva práctica, esta es una de las novedades más notables, pues los responsables y encargados del tratamiento deberán cambiar su práctica de tratamiento de datos para obedecer las nuevas normas que incluyen la implementación de políticas de protección de datos; protección de datos desde el diseño y protección de datos por defecto, la cooperación con las autoridades de supervisión (art. 30). Otras innovaciones importantes, desde la perspectiva práctica y enfocado en los responsables del tratamiento, son la inclusión del requisito de la notificación de la autoridad de control dentro de las veinticuatro horas, en caso de una injerencia en los datos personales y la notificación al interesado, si el incumplimiento afectara negativamente a su privacidad o datos personales (arts. 33 y 34), la nueva obligación de mantener la documentación de todas las operaciones de tratamiento bajo su responsabilidad (arts. 29 y 30).

[14] Asunto C-708/18, *TK v. Asociaţia de Proprietari bloc M5A-ScaraA,* STJUE de 11 de diciembre de 2019.

en el edificio, el demandante solicitaba una orden judicial para exigir la desinstalación del sistema de videovigilancia del edificio y la retirada de las cámaras instaladas en las partes comunes del mismo, argumentando que se vulneraban sus derechos a la vida privada y a la protección de datos. Ante las dudas, por parte del tribunal competente nacional, acerca de la correcta interpretación del Derecho de la UE (arts. 7, 8 y 52 CDFUE y los arts. 6 y 7 de la entonces aplicable DPD), remitió una cuestión prejudicial ante el TJUE.

Este asunto resulta relevante pues no sólo demuestra la conexión entre el derecho fundamental a la protección de datos de carácter personal y los derechos a la intimidad y a la vida privada y familiar, sino que además pone de manifiesto el carácter transversal de las garantías y derechos digitales y la relevancia del examen de ponderación que efectúa este órgano jurisprudencial europeo cuando de restricciones a derechos se trata. Este asunto versaba sobre el consentimiento del interesado (o, más bien, falta del mismo) y la instalación de un sistema de videovigilancia en las zonas comunes de un inmueble de uso residencial como restricción legítima de los derechos personalísimos ante la necesidad de garantizar la protección de las personas y bienes. A grandes rasgos, se solicitaba al TJUE, mediante cuestión prejudicial, que se pronunciara sobre la difícil conciliación de dos intereses jurídicos en conflicto enfocado en el test de necesidad: por un lado, los derechos del interesado, y por otro los intereses legítimos del responsable del tratamiento y la protección de los derechos e intereses de los demás. En palabras del propio TJUE, este debía responder «*si el establecimiento de un sistema de videovigilancia […] es proporcionado a los fines perseguidos, la cuestión de si los datos personales recogidos por dicho sistema cumplen la exigencia de proporcionalidad [exigida por la normativa de protección de datos]*»[15]. Por todo ello, los objetivos de este estudio son seis[16].

[15] *Vid*. apartado 30 de la STJUE de 11 de diciembre de 2019.

[16] (1) Explicar en detalle el caso y los elementos jurídicos relevantes que desencadenaron la controversia (los principios del tratamiento de datos especialmente relevantes, las excepciones o limitaciones al derecho fundamental a la protección de datos, el concepto jurídico indeterminado del 'interés legítimo', entre otros); (2) Estudiar en profundidad el examen y criterios de ponderación y de proporcionalidad que fija el TJUE cuando trata de conciliar derechos e intereses jurídicamente protegidos y contrapuestos; (3) Dado que el caso trata sobre limitaciones permitidas de derechos fundamentales, comentar el alcance e interpretación del art. 52 de la CDFUE a la luz de la propia jurisprudencia del TJUE en otros asuntos iusdigitales y otros parámetros en asuntos relativos a la videovigilancia fuera del ámbito laboral; (4) Analizar las consecuencias jurídicas de la doctrina emanada de esta sentencia y otras reflexiones que le surgen a la ponente en el ámbito de la protección de datos, de las situaciones derivadas de la videovigilancia privada (concretamente, en el ámbito vecinal/régimen de propiedad horizontal); (5) Cotejar el análisis hermenéutico llevado a cabo sobre el 'interés legítimo' con la jurisprudencia emanada del TJUE y los dictámenes del Comité Europeo de Protección de Datos sobre el mismo; y (6) Dado que el caso versaba todavía, por razones temporales, sobre la interpretación de la

3. ANÁLISIS DE LA SENTENCIA PREJUDICIAL: RATIFICACIÓN DE LA DOCTRINA PREVIAMENTE SENTADA Y NUEVAS APRECIACIONES JURÍDICAS

3.1. *Excepcionalidades y obviedades de partida*

Como apuntes preliminares, conviene destacar, antes de exponer la doctrina emanada de esta sentencia y nuestro correspondiente análisis jurídico, dos excepcionalidades (a expensas de una menor corrección técnica, se podría incluso decir anomalías) procedimentales (en cuanto al proceso original nacional y en cuanto al procedimiento prejudicial europeo)[17]. Por lo que nos interesa, no cabe la menor duda de que la videovigilancia, según la normativa europea de protección de datos, implica un tratamiento de datos de carácter personal. Con respecto a este caso concreto, el TJUE determina que las grabaciones videográficas (o, por sintetizar, la videovigilancia) y su almacenamiento constituyen un tratamiento de datos de carácter personal[18].

antigua normativa europea (DPD), resulta necesario comprobar y argumentar si el TJUE hubiera llegado a la misma conclusión a la luz del nuevo marco europeo de protección de datos (el Reglamento General de Protección de Datos) que, entre otras cosas, refuerza el poder de control del interesado del tratamiento e impone más obligaciones a los responsables del tratamiento de datos de carácter personal.

[17] Con esto nos referimos, por un lado, al uso de la aplicación privada (*private enfocement*) en lugar de la típica aplicación pública (*public enforcement*) del marco europeo de protección de datos. La aplicación pública del marco europeo de protección de datos por parte de las autoridades nacionales supervisoras independientes de control se considera el principal mecanismo de aplicación en materia de protección de datos. De hecho, la vía administrativa ha sido no sólo el mecanismo de preferencia, sino prácticamente la única vía de actuación para las partes interesadas en el tratamiento de datos; en el caso español, por ejemplo, primero se denuncia la presunta vulneración de las normas relativas a la protección de datos ante la Agencia Española de Protección de Datos (AEPD), en tanto autoridad independiente de supervisión y protección, y para que el asunto llegue a sede judicial, generalmente la parte en desacuerdo con la decisión de la AEPD deberá interponer recurso contencioso-administrativo contra la misma. En este caso particular, no se acudió a la autoridad independiente nacional sino directamente a los tribunales (apartado 17 de la STJUE de 11 de diciembre de 2019). Por otro lado, nos referimos también a que, en el marco del íter procesal prejudicial, este asunto se deliberó sin conclusiones del Abogado General, siendo un caso excepcional previsto en el reglamento de funcionamiento del TJUE: si el asunto no plantea ninguna cuestión de derecho nueva, se podrá dictar la decisión prejudicial (en forma de sentencia) sin conclusiones del Abogado General (art. 20 del Protocolo nº3 anexado a los Tratados constitutivos de la UE, sobre el Estatuto del Tribunal de Justicia de la Unión Europea). No concordamos del todo con esta apreciación, pues si bien el TJUE ya se ha pronunciado sobre el requisito vinculado a la prevalencia de los derechos y libertades fundamentales del interesado en la protección de datos sobre el interés legítimo perseguido por el responsable del tratamiento o por terceros interesados, en asuntos anteriores, en el que impuso la exigencia de realizar «*una ponderación de los derechos e intereses en conflicto, que dependerá de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta confieren al interesado*», sí que consideramos que existen cuestiones de especial y novedosa relevancia, las cuales expondremos más adelante. *Vid*., sobre la doctrina jurisprudencial citada, el apartado 40 de los Asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito* (ASNEFC), STJUE de 24 de noviembre de 2011. EU:C:2011:777.

[18] *Vid*. apartado 34-35 de la STJUE de 11 de diciembre de 2019.

Recordemos que, de una parte, un dato personal, para la entonces DPD, es cualquier información de una persona física identificada o identificable directa o indirectamente, y de otra parte, un tratamiento de datos personales es cualquier operación (o conjuntos de operaciones) informática(s), efectuada(s) mediante procedimientos automatizados o mecánicos, relacionadas con datos personales (desde la recogida y almacenamiento, hasta su consulta, utilización y difusión). Esto no ha cambiado sustancialmente en el nuevo marco europeo de protección de datos (el RGPD ofrece una lista *numerus apertus*, a modo ejemplificativo, de lo que puede considerarse dato personal y añade tres operaciones informáticas más de lo que constituye un tratamiento de datos de carácter personal). Así, de una lectura de la antigua DPD (aplicable a este asunto concreto) y del nuevo RGPD, no cabe la menor duda de que la grabación de imágenes, de manera continuada, y su almacenamiento en un disco duro, constituyen un tratamiento (automatizado) de datos personales.

3.2. *Interés legítimo como base jurídica para el tratamiento de datos de carácter personal: reglas y excepciones de un concepto jurídico indeterminado*

El art. 6 RGPD aborda la licitud o la legitimación del tratamiento de datos de carácter personal. Para que dicho tratamiento sea lícito, los datos personales deben ser utilizados o bien con el consentimiento del interesado o bien bajo el amparo de una base legitimadora establecida por ley (bien mediante el propio RGPD o en virtud del Derecho de la UE o de los Estados miembros en aquellos casos donde se ha permitido margen de apreciación nacional). Por lo que nos interesa, el art. 6.1 (f) RGPD establece que el: «*tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: […] el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales […]*». Adelantamos que, como bien expresa el art. 6.1 (f) *in fine* RGPD, el mero hecho de que exista un interés legítimo para el tratamiento de datos de carácter personal no quiere decir que este sea automáticamente lícito, pues será, en cualquier caso, necesario asegurar que no prevalecen otros intereses o derechos fundamentales en juego o riesgo, siendo, por tanto, necesario hacer una ponderación entre los intereses legítimos de quienes van a tratar los datos y los intereses y derechos de los titulares de los mismos para determinar cuál tendrá prevalencia.

El concepto de interés legítimo, en el ámbito de la protección de datos, ampara el tratamiento de datos de carácter personal por parte del responsable o encargado del tratamiento, sin necesidad de contar con el consentimiento del afectado (o interesado en el tratamiento); también constituye una de las bases de legitimación más ambiguas

recogidas en la normativa de protección de datos, siendo un concepto sujeto a interpretación. Así lo ha tenido que hacer en contadas ocasiones el propio TJUE. En el asunto *ASNEFC* estableció que la ponderación o evaluación que se haga requiere considerar la gravedad de la lesión de los derechos fundamentales de la persona afectada por dicho tratamiento[19]. En el asunto *Google Spain* especificó que, en el marco de esa ponderación, el derecho del interesado deberá interpretarse a la luz de los arts. 7 y 8 CDFUE[20]. En el asunto *Rigas* especificó que en lo relativo al interés legítimo de un tercero, no hay en sí una obligación de que se efectúe el tratamiento de datos sino que confiere la facultad de llevarlo a cabo y concretó los tres requisitos acumulativos para que el tratamiento de datos personales sea lícito en virtud del supuesto legitimador del art. 7(f) DPD -el ahora art. 6.1(f) RGPD-: la existencia de un interés legítimo, la necesidad y adecuación del tratamiento para alcanzar el fin legítimo y la ponderación de dicho interés con la afectación a los derechos fundamentales del interesado[21].

En el ámbito material que nos ocupa, a pesar de que la imagen grabada, en la medida en la que identifica directamente a una persona, constituye un dato de carácter personal, su tratamiento puede ser objeto para (y quedar justificado por) diversas finalidades para la satisfacción de un interés legítimo, siendo la más común, en materia de videovigilancia, la de garantizar la seguridad de las personas, bienes e instalaciones. Este no fue el caso en el asunto *Ryneš*[22], y que sí que fue el caso del asunto que abordamos en este comentario jurisprudencial; mediante el cual el Sr. TK, que se opuso, a pesar del acuerdo mayoritario por la junta de propietarios[23], de la instalación de un sistema de videovigilancia en determinadas zonas comunes del edificio. La administración del edificio aludía un interés legítimo en instalar un sistema de videovigilancia para controlar de manera más efectiva las entradas y salidas del edificio, ya que las medidas menos intrusivas tomadas con anterioridad (instalación de

[19] Asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito*, STJUE de 24 de noviembre de 2011. EU:C:2011:777.

[20] Asunto C-131/12, *Google Spain y Google*, STJUE de 13 de mayo de 2014. EU:C:2014:317

[21] Asunto C-13/16, *Rigas satiksme*, STJUE de 4 de mayo de 2017. EU:C:2017:336.

[22] Que también versaba sobre la instalación de un sistema de videovigilancia, pero en ese caso por parte de un vecino, de manera unilateral (para el cual el TJUE concluyó que no constituía una actividad exclusivamente personal o doméstica -excepción al tratamiento de datos de carácter personal de la normativa aplicable-). Vid. asunto C-212/13, *František Ryneš y Úřad pro ochranu osobních údajů,* STJUE 11 de diciembre de 2014. ECLI:EU:C:2014:2428.

[23] En el caso español, por ejemplo, puesto que se trata de la captación de imágenes en zonas comunes, la adopción de este tipo de medidas requiere, según la normativa aplicable, el acuerdo de la junta de propietarios. Para más información, se puede consultar la Guía de la AEPD sobre el uso de videocámaras para seguridad y otras finalidades (pp. 35-38). Disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-videovigilancia.pdf

un sistema de interfono y tarjeta magnética) no habían impedido los actos de vandalismo en el ascensor y en zonas comunes ni tampoco habían impedido la comisión reiterada de delitos en distintas viviendas (allanamientos y robos principalmente)[24].

También parece entenderlo el TJUE calificando de interés legítimo: «*el objetivo que persigue, en esencia, el responsable del tratamiento de los datos cuando instala un sistema de videovigilancia como el controvertido en el litigio principal, a saber, la protección de los bienes, de la salud y de la vida de los copropietarios de un inmueble*»[25]. Así, la grabación videográfica y su almacenamiento están comprendidas en uno de los supuestos legitimados por (y compatibles con) el cumplimiento de los principios de licitud, limitación de la finalidad y minimización del tratamiento[26] puesto que consideran, como intereses legítimos, la protección de los bienes, de la salud y de la vida de los copropietarios de un inmueble. Con ello queda fundamentado la concurrencia del primer requisito (la finalidad del tratamiento es legítima). A su vez, confirma que el interés legítimo perseguido no debe ser hipotético sino real, aunque no puede exigirse un perjuicio probado previo, si bien en este caso existía y ello mejor fundamenta la necesidad del sistema de videovigilancia[27]. Esto último también lo parece confirmar el Comité Europeo de Protección de Datos (CEPD), yendo, incluso un paso más allá[28].

[24] *Vid*. apartados 19 y 20 de la STJUE de 11 de diciembre de 2019.
[25] *Vid*. apartado 42 de la STJUE de 11 de diciembre de 2019.
[26] Procede subrayar que la normativa europea «*fija tres requisitos acumulativos para que el tratamiento de datos personales resulte lícito: primero, que el responsable del tratamiento o el tercero o terceros a quienes se comuniquen los datos persigan un interés legítimo; segundo, que el tratamiento de datos personales sea necesario para la satisfacción de ese interés legítimo; y, tercero, que no prevalezcan sobre el interés legítimo perseguido los derechos y libertades fundamentales del interesado en la protección de los datos*». *Vid*., en tal sentido, el apartado 40 de la STJUE de 11 de diciembre de 2019.
[27] Vid. apartado 44 de la STJUE de 11 de diciembre de 2019: «*dicho interés debe existir y ser actual en la fecha del tratamiento y no tener carácter hipotético en esa fecha. Sin embargo, a la hora de apreciar todas las circunstancias del caso no puede exigirse necesariamente que haya habido anteriormente un perjuicio para la seguridad de los bienes y de las personas*».
[28] En cuanto al l interés legítimo, este tiene quedar demostrado por la existencia de un peligro efectivo y presente, no debe ser ficticio o especulativo, y las situaciones de peligro inminente pueden constituir un interés legítimo. En cuanto a la videovigilancia, antes de iniciarla, debe existir una situación de peligro real, como daños o incidentes graves en las inmediaciones (por lo que nos interesa en materia de propiedad horizontal, concretamente habla de "las zonas que se conocen como escenarios delictivos típicos de delitos contra la propiedad"). En cuanto a justificar la base legitimadora, a la luz del principio de responsabilidad, los responsables y encargados del tratamiento harían bien en documentar los incidentes relevantes (fecha, forma, perjuicios económicos) y las acusaciones penales vinculadas a las conductas dañinas, pues la documentación de estos incidentes serán una prueba sólida de la existencia de un interés legítimo. *Vid*. Directrices 3/2019 sobre el tratamiento de datos personales mediante

Además, el TJUE considera superados los límites del examen estricto de necesidad (el alcance efectivo del interés legítimo mediante medios menos «atentatorios») puesto que medios alternativos menos intrusivos no sólo se habían aplicado con anteriores (habiendo resultados insuficientes) sino que también la medida controvertida se limitaba a las zonas comunes y vías de acceso del inmueble. Con independencia de lo anterior, sí que comparte las alegaciones de la Comisión Europea en cuanto a la posibilidad de minimizar en la medida posible el tratamiento en lo que se refiere al horario activo, a la calidad de la imagen en zonas controvertidas, entre otros aspectos que pueden minimizar el impacto en el derecho a la intimidad, a la vida privada y familiar y a la protección de datos de los residentes[29]. En esta línea también se ha pronunciado y ha dado propuestas el CEPD[30].

En efecto, el principio de minimización (junto con el de limitación de la finalidad y limitación del periodo de conservación) juega un papel esencial: se deberán recaudar sólo aquellos datos que sean necesarios o pertinentes para la finalidad concreta legítima y en una forma y durante un periodo mínimo. Por esa misma regla, no sería lícito instalar cámaras en un portal de una comunidad de propietarios cuyas grabaciones pudieran visionarse por todos los vecinos a través de un canal de televisión (a lo *Gran Hermano*) pues tampoco concordaría con el principio de proporcionalidad[31]. En el caso concreto, se pudo probar que se había procedido al borrado y a la desconexión del disco duro del sistema, que este último se había desactivado y que las imágenes grabadas habían sido eliminadas, y, con ello, quedaba absolutamente fundamentado la concurrencia del segundo requisito (el tratamiento es proporcional y necesario para la finalidad para la que se tratan los datos).

---

dispositivos de vídeo, adoptadas el 29 de enero de 2020, p. 11. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf

[29] *Vid*., los apartados 47, 49 y 51 de la STJUE de 11 de diciembre de 2019.

[30] *Vid*. Directrices 3/2019…*op.cit.,* p. 12: «*Las cuestiones relativas a la necesidad del tratamiento también surgen respecto a la forma en que se conservan las pruebas. En algunos casos puede resultar necesario utilizar soluciones de tipo «caja negra» cuando las imágenes se eliminan automáticamente después de un determinado período de almacenamiento y utilizarse únicamente en caso de producirse incidentes. En otras situaciones, puede no ser necesario registrar el material de vídeo, sino utilizar vigilancia en tiempo real en su lugar. La decisión entre optar por soluciones de tipo caja negra o la vigilancia en tiempo real también se debe basar en el fin perseguido. Si, por ejemplo, la finalidad de la videovigilancia es conservar pruebas, normalmente los métodos en tiempo real no son adecuados. En algunas ocasiones la vigilancia en tiempo real puede también ser más intrusiva que conservar y suprimir automáticamente el material, transcurrido un intervalo de tiempo determinado (p. ej., si alguien está viendo continuamente el monitor, puede ser más intrusivo que si no hay ningún monitor y el material se conserva directamente en una caja negra). El principio de la minimización de datos debe tenerse en cuenta en este contexto».*

[31] Así también se ha pronunciado la AEPD en su informe jurídico 0335/2009. Disponible en: https://www.digitalmantenimientos.com/wp-content/uploads/2011/07/Ley-Organica15-1999-proteccion-de-datos-videoportero-lopd.pdf

3.3. *Criterios de ponderación entre derechos e intereses contrapuestos: aproximación a la praxis del principio de proporcionalidad y del principio* favor libertatis *como cánones hermenéuticos*

En definitiva, y a modo de resumen, el TJUE determina que el responsable del tratamiento deberá someter las medidas que adopta, en materia de videovigilancia, al examen tripartito de proporcionalidad: a través del juicio de idoneidad (de la finalidad), del juicio de necesidad (en sentido estricto) y del juicio de proporcionalidad en sentido estricto (lo que llama la prueba de la ponderación) y hace referencia, en tanto en cuanto requiere una valoración meticulosa de la afectación individual del tratamiento de datos personales sobre la base del interés legítimo, de valorar si el interés o beneficios para el colectivo (los residentes del edificio) superan la afectación por parte del comunero que se opone.

Cabe precisar que los requisitos impuestos por la normativa europea aplicable sobre la primacía de los derechos del interesado sobre el interés o fin legítimo perseguido por el responsable del tratamiento siempre dependerá de las circunstancias concretas del caso (*case-by-case approach*), deberá interpretarse de manera sistemática con el resto del ordenamiento europeo y no de manera aislada además de que deberá tener en especial consideración la importancia de los derechos fundamentales europeos a la protección de datos y vida privada y familiar.

Sobre el examen de ponderación entre los dos intereses en juego (el tercer requisito acumulativo citado en el apartado anterior), el TJUE concluye que el criterio relativo a la gravedad de la lesión de los derechos fundamentales del interesado constituye un componente esencial de dicho ejercicio de ponderación[32] y que para este, se deben de tener en cuenta elementos tales como la naturaleza de los datos personales, el número de personas que tendrán acceso, las expectativas razonables de privacidad, entre otros[33]. Como ha explicado el CEPD, al acoger la doctrina emitida en el Dictamen 6/2014 de su sucesor, el Grupo de Trabajo del Art. 29 (GT29) sobre el concepto de interés legítimo y la interpretación del *ex* art. 7 DPD, esta ponderación o evaluación a efectos de determinar el interés legítimo no tiene que consistir en una evaluación en la que se calibran y ponderan dos intereses fácilmente cuantificables y compatibles («prueba de sopesamiento»), sino que requiere tomar en consideración factores tales como «*a) evaluación del interés legítimo del responsable del tratamiento; b) impacto sobre los interesados; c) equilibrio provisional; y d) garantías adicionales aplicadas por el responsable del tratamiento para impedir cualquier impacto indebido sobre los*

[32] *Vid*., el apartado 56 de la STJUE de 11 de diciembre de 2019.
[33] *Vid*., los apartados 57-59 de la STJUE de 11 de diciembre de 2019.

interesados»[34]. Si bien el examen de equilibrio de los intereses en jaque es obligatorio, el responsable del tratamiento tendrá que considerar cuestiones tales como el grado de afectación (y repercusiones negativas) de la videovigilancia a los intereses y los derechos y libertades fundamentales de las personas afectadas. En definitiva: «*los derechos y libertades fundamentales por un lado, y el interés legítimo del responsable por otro, deben evaluarse y equilibrarse minuciosamente*»[35].

De todo lo anterior entendemos que el órgano jurisdiccional remitente debe garantizar que los derechos y libertades fundamentales de la persona afectada por la protección de datos no prevalezcan sobre el interés legítimo perseguido. Ello requiere una ponderación de derechos e intereses opuestos, que depende de las circunstancias individuales de cada caso concreto de que se trate. El TJUE, en este caso, destaca una serie de directrices a tener en cuenta. Primero, que los Estados miembros no pueden excluir (general y categóricamente) la posibilidad de tratar determinadas categorías de datos personales sin permitir que los derechos e intereses opuestos en cuestión se sopesen entre sí en cada caso concreto. Segundo, que esta ponderación debe tener en cuenta la gravedad de la injerencia en los derechos y libertades del interesado. En este caso especifica la cuestión de si los datos proceden de fuentes públicas o no públicas (el tratamiento de datos procedentes de fuentes no públicas implica que la infracción es más grave porque la información relativa a la intimidad y vida privada del interesado será conocida a partir de entonces por el responsable del tratamiento y posiblemente por terceros). Tercero, se debe tener en cuenta, entre otras cosas, la naturaleza de los datos personales de que se trate, en particular la naturaleza de los datos, los métodos específicos de tratamiento de los datos y el número de personas que tienen acceso a los mismos. Cuarto, a efectos del ejercicio de ponderación, también son pertinentes las expectativas razonables del interesado, a saber, cuando no pueda razonablemente esperar un tratamiento ulterior de estos. Por último, todos estos elementos deben ponderarse en relación con la importancia general (para todos los copropietarios del edificio de que se trata) de los intereses legítimos perseguidos

[34] Dictamen 06/2014 de 9 de abril de 2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, pp. 39 y ss. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

[35] *Vid*. Directrices 3/2019…*op.cit.*, pp. 12-13: «*El responsable debe evaluar los riesgos de intrusión en los derechos del interesado; en este caso el criterio decisivo es la intensidad de la intervención para los derechos y libertades del particular. La intensidad se puede definir entre otros aspectos por el tipo de información que se recopila (contenido de la información), el ámbito de aplicación (densidad de la información, dimensión espacial y geográfica), el número de interesados afectados, ya sea como un número específico o en proporción a la población pertinente, la situación en cuestión, los intereses reales del grupo de interesados, los medios alternativos o la naturaleza y alcance de la evaluación de datos. Factores de equilibrio importantes pueden ser el tamaño de la zona objeto de vigilancia o la cantidad de interesados que se encuentran bajo vigilancia*».

por el sistema de videovigilancia controvertido, en la medida en que pretende esencialmente garantizar la protección de la propiedad, la salud y la vida de dichos copropietarios.

Con respecto a las expectativas razonables de privacidad, cabe al menos apuntar que el RGPD, la normativa actualmente vigente y aplicable, ahora también hace referencia a las expectativas razonables de la privacidad en el Considerando 47 aludiendo a que el interés legítimo de un responsable del tratamiento será base legitimadora para el mismo siempre y cuando no prevalezcan intereses o derechos y libertades del interesado, «*teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable*». En este sentido, recordemos tres cosas.

Primera, que, como venimos diciendo, el consentimiento del interesado no es la única base jurídica que legitima el tratamiento. Así, sería difícilmente satisfactorio el argumento que no se sabía sobre la instalación de dicho sistema si se aprobó (con la oposición del interesado del tratamiento) en la junta, llegando al quorum necesario en virtud de la normativa aplicable cuando se trata de cuestiones relativas al establecimiento de servicios de portería, conserjería y vigilancia[36]. Segunda, y en cualquier caso, que el interesado, cuyos datos son objeto de tratamiento, debe tener derecho a saber qué datos personales se están tratando, cómo, cuándo, dónde, por qué y quién tiene acceso a ellos, así como para qué finalidades se están usando y oponerse por razones legítimas. Y tercera, y subsiguientemente, que el responsable del tratamiento deberá asegurar que existe un distintivo de zona videovigilada, ubicado en un lugar suficientemente visible, en el que también deberán constar determinados elementos con el fin de dar cumplimiento a las obligaciones de información y transparencia.

En general, con respecto al principio de proporcionalidad como canon hermenéutico, el TJUE reconoce que en materia de protección de datos y cuando se trata de la ponderación de intereses y derechos en conflicto en casos *iusdigitales*, el art. 8 y el art. 52 de la CDFUE deberán interpretarse de manera conjunta. Recordemos que el art. 52 CDFUE reza que cualquier limitación a los derechos reconocidos en la misma (incluido el derecho fundamental y autónomo a la protección de datos reconocido en el art. 8) «*deberá estar establecida por la ley y respetar el contenido esencial de dichos derechos y libertades*», pudiéndose únicamente introducir limitaciones cuando respeten el

[36] Según el art. 17.3 de la Ley de Propiedad Horizontal (con las modificaciones efectuadas tras la entrada en vigor de la Ley 8/2013, de Rehabilitación, Regeneración y Renovación urbanas), este quorum se alcanzaría con la mayoría cualificada; es decir, las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación.

principio de proporcionalidad «*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*».

En particular, con respecto a la evaluación de la necesidad de la medida, cabe interpretar que, ateniendo a los criterios que fija, el TJUE en todo momento hace alusión a un test de necesidad estricto, al igual que hizo con otros asuntos en materia de protección de datos en los que había que ponderar los derechos y libertades de los interesados del tratamiento, como, por ejemplo, en el asunto *Digital Rights Ireland*[37].En este asunto el TJUE introdujo un examen de control estricto, a través de un test de proporcionalidad riguroso de los actos legislativos de la Unión que interfieren ponderadamente con los derechos a la vida privada y a la protección de datos de carácter personal, concluyendo que la mera obligación de conservación de datos de carácter personal era, por sí sola, una injerencia tanto en el derecho a la vida privada como en el derecho a la protección de datos, calificándolas de grandes, graves y generadoras de un sentimiento de que la vida privada es objeto de una vigilancia constante. En el caso que nos ocupa, el TJUE enfatiza que el tratamiento debe aplicarse sólo en la medida en que sea estrictamente necesario, lo que significa que en un primer momento debieron aplicarse medidas alternativas que finalmente resultaron ser insuficientes y que la propia naturaleza del tratamiento y de su almacenamiento debían ser reducidas a la mínima expresión posible para alcanzar el objetivo.

Asimismo, ateniendo a las consideraciones supramencionadas y a los criterios que fija, podríamos decir que TJUE también insinúa el potencial uso de otro criterio hermenéutico, el llamado principio *favor libertatis* o *pro personae*[38], a la hora de ponderar derechos e intereses en el contexto de limitaciones o excepciones al ejercicio de los derechos y garantías del interesado[39]. Este, a fin de cuentas, actúa como criterio

[37] Asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd v. Seitlinger y otros,* STJUE de 8 de abril de 2014, ECLI:EU:C:2014:238.

[38] Se entienda bien como «preferencia interpretativa», es decir, como principio interpretativo en sí mismo, buscando establecer una vía interpretativa específica, o como "preferencia de normas", es decir, como técnica resolutiva de conflictos entre normas, buscando establecer una solución ante un choque entre normas concernientes a derechos fundamentales. Vid. Carpio Marcos, E., *La Interpretación de los Derechos Fundamentales*, Lima, Palestra editores, 2004, pp. 470-473; o más recientemente, Rodarte Berbera, H., «The Pro Personae Principle and its Application by Mexican Courts». *Queen Mary Human Rights Law Review*, *4*(1), 2017, p. 10.

[39] Aludiendo a lo que ahora el RGPD llama «la situación particular del interesado» y lo que ha sido objeto de estudio en otro lugar con respecto a situaciones de vulnerabilidad socio-digital. *Vid*. Martínez López-Sáez, M., *La garantía del derecho al olvido: protección de datos, retos futuros y propuestas de regulación de situaciones de vulnerabilidad en la Unión Europea* (Tesis Doctoral). Universidad de Valencia, 2020.

interpretativo informador, bajo un enfoque basado en los derechos humanos, pues en caso de que existan diversas interpretaciones posibles respecto de una norma o medida que pueda generar afectaciones a un derecho, el principio *favor libertatis* establece que debe hacerse una interpretación extensiva del alcance y ejercicio de los derechos y, correlativamente, una interpretación restrictiva de sus limitaciones. Empero, es cierto que en ocasiones la aplicación del principio *favor libertatis* puede derivar en una «paradoja" difícilmente salvable[40], si nos referimos al caso de conflictos entre derechos y libertades en el que debe efectuarse una ponderación; sobre todo, en el caso de conflictos *drittwirkungianos* en tanto las personas son titulares de los mismos (los comuneros tienen tanto derecho a la protección de datos y a la intimidad personal y familiar como a la seguridad e integridad física y a la propiedad privada, y estos bienes jurídicos protegidos pueden verse contrapuestos en situaciones de videovigilancia residencial).

No obstante lo anterior, como hemos podido apreciar de la última exégesis jurisprudencial del TJUE, el principio *favor libertatis*, en casos *iusdigitales*, se ha aplicado sistemáticamente a favor del derecho a la protección de datos y sus valores axiológicos subyacentes (intimidad, privacidad, honor, reputación, integridad moral, etc.). Ello se ha hecho estableciendo, aunque tímidamente al principio, que aunque este derecho (y sus garantías –como era el derecho al olvido-) no son absolutos, sí que pueden tener carácter preferente sobre el interés del público a conocer la información personal y sobre otros intereses «legítimos" del responsable del tratamiento siempre y cuando no exista un justificado interés preponderante y esencial[41].

También ha establecido que, para datos especialmente sensibles, se requerirá también de límites que respeten su contenido esencial[42] y que superen un examen estricto de proporcionalidad, y, como último elemento garante, determinando su prevalencia en circunstancias excepcionales ateniendo a la situación particular del interesado y permitiendo modulaciones en virtud del principio de minimización del tratamiento, entre otros[43]. Podríamos resumir las reglas ponderativas del TJUE en estos casos, en

[40] Negishi, Y., «The Pro Homine Principle's Role in Regulating the Relationship between Conventionality Control and Constitutionality Control», *European Journal of International Law*, *28*(2), 2017, p. 479.

[41] Establecido por primera vez en el supracitado asunto *Google Spain*, y luego referenciado en los asuntos *Google LLC v. CNIL* (Asunto C-507/17, STJUE de 24 de septiembre de 2019) y *GC y Otros v. CNIL* (Asunto C-136/17, STJUE de 24 de septiembre de 2019).

[42] Recordemos que, en caso de dudas de cómo equilibrar la balanza a través de la doctrina normativa y jurisprudencial europea, debemos de acudir a las pautas que marcan la CDFUE con relación a las limitaciones relativas a los derechos fundamentales del art. 52.1 CDFUE, teniendo su equivalente en el marco hermenéutico del TEDH sobre el conflicto entre la vida privada y la libertad de expresión.

[43] Establecido por primera vez en el asunto *Manni (*Asunto C-398/15, STJUE de 9 de marzo de 2017) y detallándolo y añadiéndole en el asunto *GC y Otros v. CNIL.*

virtud del principio *favor libertatis* (o mejor dicho, *pro personae*) bajo las siguientes máximas: injerencia grave en los derechos, datos sensibles, expectativa de privacidad crecientes-interés legítimo menguante. En análoga línea, cabe recordar que este principio se fundamenta en criterios substantivos y «*en el proceso a quo*»[44], aludiendo, de nuevo, al *case by case defence* por la que siempre se ha decantado el TJUE, por lo que tendremos que estar a las situaciones específicas del caso (por ejemplo, a la medidas tomadas para minimizar el tratamiento de datos y la situación particular del interesado del tratamiento, entre otros factores).

4. RELEVANCIA PARA EL DERECHO INTERNO: LA PROTECCIÓN DE DATOS A LA LUZ DE UN SISTEMA MULTINIVEL DE DERECHOS Y DE UN REGLAMENTO CON EXCESIVO MARGEN DE APRECIACIÓN NACIONAL

Además de que la jurisprudencia del TJUE es vinculante, en cuanto intérprete máximo del Derecho de la UE (incluido la CDFUE como parte del derecho originario y el derecho derivado de la competencia legislativa general y específica conferida por el art. 16 TFUE en materia de protección de datos), esta sentencia es relevante para el ordenamiento jurídico español por diversas razones. En efecto, aunque el TJUE era el competente para resolver esta duda, en cuando interprete supremo del Derecho de la UE como derecho aplicable al caso controvertido, la decisión prejudicial emitida tras una cuestión prejudicial de interpretación deja al órgano jurisdiccional nacional la decisión última de cómo resolver *(*«*Corresponde al órgano jurisdiccional remitente comprobar […]*»; lo que potencialmente da luz verde a criterios diferentes.

Aunque esta sentencia trataba todavía sobre el antiguo marco normativo (DPD) y versaba sobre el Derecho rumano, es necesario advertir de las consecuencias jurídicas significativas derivadas de las llamadas clausulas abiertas/de flexibilidad que siguen existiendo en el actual marco normativo (RGPD) y su relación con el caso controvertido en virtud de su adaptación normativa nacional española (en especial en las «Disposiciones aplicables a tratamiento concretos» del Título IV de la nueva Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales)[45] y otras cuestiones jurídicas en el marco del Derecho Constitucional.

[44] Rolla, G., «La tutela directa de los derechos fundamentales por los tribunales constitucionales», *Anuario Iberoamericano de Justicia Constitucional*, 11, 2007, p. 325.

[45] El fenómeno de las llamadas clausulas «abiertas» o de «flexibilidad», todavía poco común (aunque cada vez más visto) en los reglamentos europeos, hace del RGPD un acto directamente aplicable y jurídicamente vinculante un tanto especial. Se aprecian ciertas especificidades y margen de apreciación nacional al enunciar el RGPD que los ordenamientos jurídicos de los Estados miembros podrán, en la medida en que sea necesario por motivos de coherencia normativa, incorporar elementos adicionales o restricciones al mismo cuando este lo permita (Considerando 8 RGPD). En el Capítulo IX (arts. 85 a 91) del RGPD, sin lugar a dudas, deja margen de discrecionalidad nacional para fragmentar las garantías

Partiendo de la premisa de que nos movemos en un momento de proliferación de los derechos, nos encontramos ante una necesaria y relativa conciliación entre derechos relativos en conflicto, con los problemas inherentes que plantea dicha ponderación. La normativa europea en materia de protección de datos ha establecido que, cuando de injerencias en los derechos de terceros se trata, es necesario efectuar el supracitado examen entre ellos. Los límites del derecho a la protección de datos (al igual que con sus garantías jurídicas llamadas derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación, como contenido positivo de dicho derecho fundamental) precisamente aluden a ese equilibrio entre derechos e intereses pues la normativa europea circunscribe límites a su pleno y efectivo ejercicio cuando el tratamiento resulta necesario, entre otras razones, para alcanzar un fin legítimo o imperioso por parte o cuenta del responsable del tratamiento. En función de las razones específicas y justificadas durante el examen de ponderación de los intereses en juego, se inclinará la balanza a favor de un derecho/interés u otro, no existiendo derechos absolutos ni invalidaciones automáticas.

Una vez analizado el juicio de ponderación en el marco de afectaciones al derecho fundamental a la protección de datos, cabe también aludir la vía más común en estos ámbitos (la civil) pues quedan también afectados los derechos a la imagen, a la intimidad, y a la vida privada y familiar (constitucionalmente reconocidos y desarrollados en la Ley Orgánica 1/1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen). Según algunos autores, en materia de videovigilancia en el ámbito residencial «*será necesario ponderar los bienes jurídicos protegidos, que no son otros, generalmente, que la seguridad de las personas y/o bienes de los componentes de la comunidad y su intimidad. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otras medidas menos intrusivas de la intimidad de las personas*»[46]. Asimismo, con respecto al derecho a la propia imagen, directamente afectado por la grabación videográfica, también hay que tener en cuenta la existencia de un riesgo real (constatado por actos previos documentados), entre

básicas del derecho fundamental a la protección de datos de los interesados, precisamente por permitir la imposición de restricciones adicionales a los derechos que él mismo reconoce (acceso, supresión, oposición y limitación, en particular). En su adaptación normativa esto se ve en determinados ámbitos sectoriales. Por ejemplo, en materia de videovigilancia (art. 22 LOPDGDD), sea privada o pública, la norma española se acoge al margen de maniobra nacional que permite el art. 23.1(c) y (d) RGPD, mediante la posibilidad de restringir el ejercicio o alcance de los derechos del interesado para salvaguardar bienes e intereses jurídicamente protegidos; lo que en otros supuestos también ha denominado intereses legítimos. Una explicación resumida de las cuestiones supracitadas se encuentra disponible en: https://www.iberley.es/temas/tratamiento-datos-fines-videovigilancia-62854

[46] Díaz Martínez, A., «Honor. Intimidad y protección de datos personales en las comunidades en régimen de propiedad horizontal». *Derecho privado y Constitución*, *32*, 2017, p. 234.

otros factores podrán suponer que la adopción de medidas de videovigilancia respete los limites acordados en la LO 1/1982 y no se estima infringido.

Mendoza apunta que, por razones obvias, en el caso de tratamiento de datos recopilados mediante sistemas de videovigilancia, solo tiene sentido reconocer (y asegurar el ejercicio de) el derecho de acceso y no el derecho de rectificación u oposición, pues estos resultarían incompatibles con la finalidad perseguida por la instalación del sistema[47]. Sin embargo, cabe recordar dos apreciaciones. Por un lado, que ciertos derechos sí que podrían ser perfectamente ejercitados, como por ejemplo el de supresión que está íntimamente ligado a los principios de minimización y de limitación del periodo de conservación (si alguno de los supuestos habilitadores para su ejercicio fuera aplicable y no hubiera razones de interés imperioso, por razones de interés público o permitir ejercitar acciones judiciales, el responsable del tratamiento tendría 1 mes para la supresión de la grabaciones[48]). Es decir, solo se conservarán más tiempo cuando haya que aportar la imagen como prueba. Por otro lado, también sería de aplicación, mientras el responsable del tratamiento determina si existe un interés legítimo o si existen razones fundadas y establecidas en el RGPD para borrar la grabación cuando reciba una solicitud de supresión, ejercer el derecho a la limitación del tratamiento como medida cautelar[49].

Repárese en que los requisitos acumulativos vinculados al examen de la legitimidad del interés perseguido por el responsable del tratamiento (que, en consecuencia, limita, entre otros derechos, el de la protección de los datos de carácter personal), recuerdan el triple test utilizado por el TEDH para ponderar las restricciones que se recogen en algunas disposiciones del CEDH (entre ellas, el art. 8, que reconoce el derecho a la vida privada y familiar, mediante el cual, el TEDH también ha consagrado el derecho a la protección de datos), a saber, que estén previstas legalmente, persigan un fin legítimo y sean necesarias en una sociedad democrática en clave de proporcionalidad. Todo esto también lo ha asumido la jurisdicción española. En sede extraordinaria, el Tribunal Constitucional también se ha pronunciado. Puesto que la instalación de cámaras de videovigilancia choca frontalmente con un derecho fundamental, especialmente ligado a los clásicos derechos personalísimos, su instalación debe hacerse respetando el principio de proporcionalidad. Este principio jurídico indeterminado ha sido ya

[47] Mendoza Losana, A., *Derechos y obligaciones de los propietarios que instalan cámaras de seguridad en sus viviendas.* Blog Centro de Estudios de Consumo-UCLM, 2015.

[48] Art. 17 RGPD. Vid., para un desarrollo más exhaustivo, Martínez López-Sáez, M., *La garantía del derecho al olvido…op.cit.*

[49] Art. 19 RGPD. Su ejercicio lo trata Martínez López-Sáez, M., «El derecho a la limitación del tratamiento en el RGPD: balance de su acomodación normativa en la LOPDGDD», Ponencia en el *Congreso Internacional RGPD en España*, Universidad Jaime I, Castellón de la Plana, 2021.

abordado por nuestro Tribunal Constitucional (TC), afirmando que este es «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales»[50].

En este sentido, el TC ha concluido que cualquier medida restrictiva de derechos y libertades fundamentales, entre las que cabe incluir, por supuesto aquellas que supongan una injerencia en los derechos a la integridad física y a la intimidad deberá guiarse por una estricta observancia del principio de proporcionalidad (recordemos que así también se ha consagrado en el art. 52 de la CDFUE y lo ha interpretado el TJUE). Y lo anterior se dará, según el propio TC, cuando se den tres requisitos o condiciones: «*si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)* »[51].

En sede ordinaria, cabe destacar que ha habido casos en los que se ha considerado que quedaba superado el juicio de idoneidad (porque las personas que han producido o puedan producir daños en el futuro en el portal del inmueble conocerían que podrían ser identificadas a través de la grabación, como efecto disuasorio), el juicio de necesidad (porque la instalación del sistema de videovigilancia era el más operativo para impedir que se siguieran produciendo daños en el inmueble, o en caso de producirse, que permitiera identificar a los autores) y el juicio de proporcionalidad (por derivarse de la medida más beneficios para el conjunto de los propietarios que perjuicios para ello o terceros)[52]. En otros, aunque con hechos no análogos, como es el caso de la instalación de cámaras de videovigilancia falsas por un vecino, también ha conllevado a juicios de proporcionalidad bien distintos. Por ejemplo, la duda razonable de estar siendo observando en un ámbito privado con este tipo de dispositivos por parte de otros vecinos, es susceptible de coartar su libertad y un impedimento desproporcional en el disfrute de su derecho a la intimidad[53].

[50] Vid., por todas, en su STC 207/1996 de 16 de diciembre (FJ 4 *in fine*).
[51] *Id*.
[52] *Vid*. SAP Coruña 25 marzo 2009.
[53] *Vid*. STS de 7 de noviembre de 2019. pudiendo suplir, en ocasiones, los mecanismos de protección previstos en la LO 1/1982 las pretensiones de aquellos interesados del tratamiento que quedan no pueden acudir por la vía administrativa (al no haber grabación, no hay un tratamiento de datos personales, pero sí una injerencia en derechos íntimamente vinculados).

5. CONCLUSIONES

Suponiendo que la videovigilancia sea necesaria para proteger los intereses legítimos de un responsable, un sistema de videovigilancia solo podrá emplearse si los intereses legítimos del responsable o los de un tercero (p. ej., protección de la propiedad o de la integridad física) prevalecen sobre los intereses o los derechos y las libertades fundamentales del interesado. En el caso concreto, la DPD, y nosotros afirmamos que también el RGPD[54], no impide la instalación de un sistema de videovigilancia para proteger la propiedad, la salud y la vida de los comuneros de un edificio de viviendas por ser esta finalidad un interés legítimo y haberse superado el test de necesidad.

Se podrían realizar, como corolario, tres conclusiones principales. Primeramente, al igual que otros conceptos jurídicos indeterminados en materia de protección de datos, el «interés legítimo del responsable del tratamiento», no sólo constituye una base jurídica consagrada para la legitimación del tratamiento (sin requerir el consentimiento del interesado) en determinados supuestos, sino que también constituye un criterio legitimador y ampliamente recurrido que tiene como consecuencia directa la imposibilidad de ejercer un control absoluto y efectivo de los datos de carácter personal, atentando contra el derecho a la protección de datos y otros derechos y libertades fundamentales en especial riesgo por la innovación tecnológica y la transformación digital. En determinados casos, esta prevalencia en algunos de los supuestos tiene cierto sentido y denota buen criterio pues pretenden preservar determinados principios generales del Derecho, otros bienes e intereses jurídicamente protegidos, y los propios derechos del interesado. Sin embargo, en otros casos, tiene menos sentido, sobre todo cuando se trata de ámbitos en los que las relaciones jurídicas nacen de por sí desequilibradas o las consecuencias negativas (o daños e injerencia en otros derechos fundamentales) son más notables y más irreversibles.

A continuación, en segundo lugar, en el examen de proporcionalidad tendente a justificar, en materia de videovigilancia, la medida/tratamiento amparada/o por el interés legítimo, el TJUE implanta un examen de necesidad más estricto de lo habitual, que exige tener en cuenta no sólo el principio de proporcionalidad (como criterio hermenéutico), sino también, como parte sustancial del test de necesidad, el principio de minimización del tratamiento. Esto ha permitido limitar el amplio margen de discrecionalidad que se le permitía al responsable del tratamiento pues ya no sólo hay que probar que los fines legítimos no puedan alcanzarse con igual eficacia por otros

[54] Aunque este caso se resolvió bajo el régimen anterior de protección de datos (siendo aplicable la DPD), es muy probable (por no decir seguro) que se apliquen razonamientos y conclusiones similares bajo el RGPD pues ni disposición normativa ni los principios de protección de datos han cambiado.

medios menos atentatorios contra los derechos personalísimos clásicos o emergentes supracitados (en otras palabras, que no existe una alternativa menos restrictiva o lesiva), sino también asegurarse que el modo concreto de la instalación, su funcionamiento y el propio tratamiento están lo más limitado posible para alcanzar dicho objetivo (lo que requiere imponer límites, por diseño y por defecto, a la instalación, al funcionamiento y al tratamiento para asegurar la licitud y proporcionalidad del mismo).

Por último, que se considere que un sistema de videovigilancia realiza un tratamiento lícito de datos de carácter personal (como es la imagen de una persona), deben cumplirse tres condiciones. La última de estas es, a nuestro parecer, la más interesante pues parece estar inspirada en el principio *favor libertatis* (o *pro personae*), que se demuestre que no existen derechos o libertades individuales que prevalecen sobre el interés legítimo perseguido. Para ello, el TJUE proporciona razones y pautas a tener en cuenta relacionadas con la situación particular del interesado, con el ejercicio de los derechos ARSOPOL, con la naturaleza de la información personal recabada o directamente con la gravedad de la lesión de los derechos afectados.

En definitiva, la instalación de sistemas de videovigilancia debe tener como fin principal el evitar determinadas situaciones de inseguridad para los residentes para constituir un fin legítimo y ha de ser una medida proporcional en relación con el riesgo o daño que se pretende evitar y en cualquier caso debe ser siempre un recurso subsidiario. Todo lo anterior obligará, en el marco de los sistemas de videovigilancia, a hacer una evaluación seria del interés legítimo y de los riesgos para los derechos fundamentales (análogas a las archiconocidas y diversas evaluaciones de impacto ya existentes en materia de protección de datos y las clásicas de la técnica legislativa).

BIBLIOGRAFÍA

CARPIO MARCOS, E., *La Interpretación de los Derechos Fundamentales,* Lima, Palestra editores, 2004.

DÍAZ MARTÍNEZ, A., «Honor. Intimidad y protección de datos personales en las comunidades en régimen de propiedad horizontal*» Derecho privado y Constitución*, *32*, 2018, 187-245.

GARCÍA, A.: "Cámaras de videovigilancia en el edificio con la oposición de alguno de los vecinos", *Inmueble: Revista del sector inmobiliario, 189*, 2019, 16-20.

GARCÍA MAHAMUT, R., «Del Reglamento General de Protección de Datos a la LO 3/2018 de Protección de Datos Personales y Garantías de los Derechos Digitales» En R. García Mahamut, y B. Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales,* Valencia, Tirant Lo Blanch, 2019, pp. 95-131

MARTÍNEZ LÓPEZ-SÁEZ, M., «El derecho a la limitación del tratamiento en el RGPD: balance de su acomodación normativa en la LOPDGDD». Ponencia en el *Congreso Internacional RGPD en España*, Universidad Jaime I, Castellón de la Plana, 2021.

MARTÍNEZ LÓPEZ-SÁEZ, M., *La garantía del derecho al olvido: protección de datos, retos futuros y propuestas de regulación de situaciones de vulnerabilidad en la Unión Europea* (Tesis Doctoral), Universidad de Valencia, 2020.

MARTÍNEZ LÓPEZ-SÁEZ, M., «Repensando el Derecho Constitucional a la Protección de Datos ante la Mutación de la Informática», En J. Martín Cubas (Ed.), *Repensando la Constitución 40 años después* (pp. 147-160), Valencia, Tirant Lo Blanch, 2019.

MARTÍNEZ LÓPEZ-SÁEZ, M., «Hacia una integración digital europea: la constitucionalización del derecho de la UE y la europeización del Derecho Constitucional en materia de protección de datos». *Revista de Estudios Europeos*, *71*, 2018, pp. 23-37.

MENDOZA LOSANA, A., *Derechos y obligaciones de los propietarios que instalan cámaras de seguridad en sus viviendas.* Blog Centro de Estudios de Consumo-UCLM, 2015. Recuperado de: https://blog.uclm.es/cesco/files/2015/02/Derechos-y-obligaciones-de-los-propietarios-que-instalan-c%c3%a1maras-de-seguridad-en-sus-viviendas.pdf

MURILLO DE LA CUEVA, P.L., «El Tribunal Supremo y el derecho a la protección de datos» En R. García Mahamut, y B. Tomás Mallén (Eds.), *El Reglamento General de Protección de Datos un Enfoque Nacional y Comparado. Especial Referencia a la LO 3/2018 De Protección de Datos y Garantía de los Derechos Digitales,* Valencia, Tirant Lo Blanch, 2019, pp.181-207.

NEGISHI, Y., «The Pro Homine Principle's Role in Regulating the Relationship between Conventionality Control and Constitutionality Control». *European Journal of International Law*, *28*(2), 2017, pp. 457–481.

RALLO LOMBARTE, A., «Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma». *Revista de Derecho Político (UNED), 85*, 2012, pp. 13-56.

RODARTE BERBERA, H., «The Pro Personae Principle and its Application by Mexican Courts». *Queen Mary Human Rights Law Review*, *4*(1), 2017, pp. 1-27.

RODOTÀ, S., *El derecho a tener derechos.* (trad. Revuelta López, J.), Bolonia, Trotta, 2014.

ROLLA, G., «La tutela directa de los derechos fundamentales por los tribunales constitucionales*»*. *Anuario Iberoamericano de Justicia Constitucional*, 11, 2007, pp. 301-326.

ZUBOFF, S., *The Age of Surveillance Capitalism,* London, Profile Books Ltd, 2019.

FECHA DE RECEPCIÓN: 11.07.2022

FECHA DE ACEPTACIÓN: 05.12.2022