RGPD y actividades personales en materia de protección de datos

RGPD and personal activities in the field of data protection

Jorge Justo Megías Quirós
Universidad de Cádiz
https://orcid.org/0000-0002-2245-7971
josejusto.megias@uca.es

RECIBIDO: 02/07/2019 / ACEPTADO: 01/11/2019

Resumen: Los avances tecnológicos han facilitado el tratamiento de datos personales por parte de los particulares, lo que puede suponer un mayor riesgo para la protección de la privacidad. Este estudio analiza la excepción doméstica contemplada en los textos normativos, comunitarios y nacionales, y la consiguiente exclusión de las actividades personales y domésticas del ámbito de aplicación de las normas de protección de datos. Ofrece la respuesta de los tribunales y de la AEPD a los supuestos más conflictivos.

Palabras clave: protección de datos, actividad personal, excepción doméstica, web, red social, videovigilancia, dron, cámara *on board*.

Abstract: Technological advances have facilitated the processing of personal data by individuals, which may pose a greater risk for the protection of privacy. This study analyzes the domestic exception contemplated in normative texts, community and national, and the consequent exclusion of personal and domestic activities from the field of application of data protection regulations. It offers the response of the courts and the AEPD to the most conflicting cases.

Keywords: data protection, personal activity, domestic exception, web, social network, video surveillance, drone, camera on board.

1. Introducción

El conocimiento de un dato personal aislado de fácil acceso público (nombre, imagen, haber estado en un lugar, haber desarrollado una acción determinada, etc.) puede resultar inocuo, pero, combinado con otros datos, puede revelar el perfil de la persona, o, difundido en determinados medios, puede conllevar consecuencias indeseadas para su titular. Los avances tecnológicos no sólo permiten obtener estos datos con gran facilidad, sino también un tratamiento y difusión tan sencilla que, si no se establecieran protecciones, la vulnerabilidad de la vida privada de la persona sería constante. De ahí la relevancia del derecho a la autodeterminación informativa que complementa la vertiente negativa del

derecho a la intimidad[1]. Éste permite excluir a los extraños del conocimiento de nuestros datos íntimos, mientras que aquél nos otorga positivamente el control sobre nuestros datos personales, garantizando «un poder de control sobre los datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»[2].

Para garantizar este poder de control se aprobaron en los años 90 normas de ámbito comunitario y nacional en las que se regulaba estrictamente el tratamiento de los datos de carácter personal, pero todas ellas contemplaban en su articulado ciertas excepciones –tratamientos no sujetos a sus ámbitos de aplicación–, entre las que se encuentra la que va a ser objeto de este estudio: los tratamientos realizados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Hasta fechas recientes, era la 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 los datos personales y a su libre circulación, la que establecía el marco comunitario al que debían ajustarse las regulaciones nacionales de la UE[3]. Desde mayo de 2018, fecha en la que entró en vigor, contamos con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[4], conocido como Reglamento General de Protección de Datos (RGPD).

---

1 El Convenio Europeo de Derechos Humanos (1950) sólo reconocía en su artículo 8.1 el derecho al respeto de la vida privada y familiar («toda persona tiene derecho al respeto de la vida privada y familiar, de su domicilio y de su correspondencia»), lo que hizo necesaria la posterior protección de los datos de carácter personal mediante el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (y su Protocolo Adicional de 8 de noviembre de 2001). La Carta de los Derechos Fundamentales de la UE reconoce tanto el derecho al respeto de toda persona «a su vida privada y familiar» (art. 7) como el derecho «a la protección de los datos de carácter personal que la conciernan» (art. 8).

2 STC 292/2000, de 30 de noviembre, FJ 6º (ECLI:ES:TC:2000:292). Las garantías de este poder son más estrictas en la medida en que la sensibilidad del dato es mayor, pues no es lo mismo difundir un nombre o una dirección que revelar datos referidos al origen racial o étnico, ideología, creencias, afiliación sindical, salud o vida sexual.

3 En el ámbito nacional contábamos, al margen de otras normas sectoriales, con la LO 15/1999 de Protección de Datos y el RD 1720/2007, que aprobó su Reglamento de Desarrollo. Desde diciembre de 2018 contamos con la nueva LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD), que en la materia que nos ocupa no ha introducido modificación alguna.

4 DOUE L 119, de 4 de mayo de 2016, pp. 1-88.

El nuevo RGPD, como puso de manifiesto la propia Comisión Europea, «no ha modificado de manera sustancial los conceptos y principios básicos de la legislación en materia de protección de datos establecida en 1995»[5]. Sin embargo, debemos matizar que en algunos aspectos los cambios introducidos por el RGPD sí son relevantes (consentimiento, delegado de protección de datos, sustitución de la autorización por control, etc.), aunque, en lo que atañe a la excepción que nos ocupa, es cierto que no se ha producido cambio sustancial, permaneciendo idénticas las redacciones del artículo 3.2 de la Directiva derogada y el nuevo artículo 2.2.c) RGPD, que continúa excluyendo de su ámbito de aplicación todo tratamiento de datos personales «efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas». Sin embargo, el tipo de norma elegido –Reglamento en lugar de Directiva– sí que podrá influir en la práctica dada su aplicación directa en todos los Estados y, sobre todo, por la limitación de la interpretación que se pueda hacer de su contenido. La Comisión ha advertido a los legisladores nacionales en su *Comunicación COM(2018) 43 final* que «la interpretación del Reglamento compete a los órganos jurisdiccionales europeos (los tribunales nacionales y, en última instancia, el Tribunal de Justicia Europeo) y no a los legisladores de los Estados miembros»[6], correspondiendo al nuevo Comité Europeo de Protección de Datos –sucesor del Grupo de Trabajo del artículo 29 (GT29)– emitir los dictámenes oportunos cuando sea necesario[7].

---

5 Añade a continuación que «esto debería significar que la gran mayoría de los responsables y encargados del tratamiento, siempre que cumplan ya la legislación vigente de la UE en materia de protección de datos, no necesitarán realizar cambios importantes en sus operaciones de tratamiento de datos para cumplir el Reglamento». Comunicación COM(2018) 43 final, de 24 de enero de 2018, de la Comisión al Parlamento Europeo y al Consejo, Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018, p. 12.

6 Comunicación COM(2018) 43 final, p. 10. Previamente había manifestado, en aras de la unidad en todo el territorio UE, que «ya que es fundamental que los operadores dispongan de un conjunto de orientaciones único y coherente, las directrices actuales a nivel nacional deben derogarse o adaptarse a las adoptadas por el Grupo de trabajo del artículo 29 o el Comité Europeo de Protección de Datos sobre el mismo tema» (p. 8).

7 También la propia Comisión podrá orientar «en la mejor comprensión de las normas de protección de datos de la UE, pero únicamente el texto del Reglamento tiene validez jurídica. En consecuencia, sólo el Reglamento puede generar derechos y obligaciones para los individuos». Comunicación COM(2018) 43 final, p. 14, nota 48. Por lo que respecta a la normativa española, la nueva LOPD se limita a admitir en el art. 2.2.a) la excepción doméstica con una remisión explícita al RGPD.

Así, pues, como principio general, podemos afirmar que el tratamiento de datos personales propios y ajenos realizado por una persona física no estará sujeto a las exigencias del RGPD cuando se trate de actividades exclusivamente personales o domésticas –aunque se hayan desarrollado en espacio público– con una finalidad privada[8]. La justificación de la excepción se encuentra en el fin último perseguido por la regulación, que es garantizar el derecho a la vida privada de los ciudadanos y al control de sus datos de carácter personal. Si, por un lado, sería paternalismo imponer a los ciudadanos obligaciones de control sobre los datos *propios* generados en la esfera personal, familiar o de amistad[9], por otro, sería excesivo imponer un control de los tratamientos de datos *ajenos* (fotos, vídeos, nombres, direcciones, teléfonos...) cuando tales tratamientos afecten mínimamente a la vida privada de los terceros implicados, como ocurre en los realizados por un particular en el curso de actividades personales y domésticas y se circunscriben a estas esferas. Así, pues, quedarían excluidos del ámbito de aplicación del RGPD, por ejemplo, los directorios o agendas personales, los álbumes de fotos familiares y amistades, los registros de contabilidad familiar, los vídeos domésticos, los listados para invitaciones de celebraciones familiares o de amistad, etc., cuando no sean utilizados para una finalidad que exceda su cometido original. Si estos ficheros fueran, por ejemplo, difundidos en una red social sin limitación de acceso, o utilizados con fines comerciales, o en procedimientos judiciales, ya no les sería de aplicación la excepción doméstica contemplada por el RGPD[10].

---

8 El RGPD recoge de modo implícito la insistencia del Supervisor Europeo de Protección de Datos en que todo tratamiento no sólo debe tener base legal, sino también finalidad justificada: «Las exigencias con arreglo a las que todo tratamiento de datos ha de limitarse a una finalidad concreta y basarse en un fundamento jurídico son acumulativas, no alternativas». *Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos*, de 20 de julio de 2015, p. 3 (DOUE C 301, pp. 1-8).

9 A ello se refiere el Grupo de trabajo del artículo 29 en su Dictamen 4/2007 sobre el concepto de datos personales, WP 136, adoptado el 20 de junio de 2007, cuando destaca la flexibilidad conferida al texto de la Directiva 95/46/CE para buscar sin rigideces y sin maximalismos la solución adecuada a cada caso. Por ello, «Un resultado no deseado sería el de terminar aplicando las normas de protección de datos a situaciones que, en principio, no deberían estar cubiertas por estas normas; y para las que no fueron concebidas por el legislador. Las exenciones sustanciales previstas en el artículo 3 mencionado anteriormente y las aclaraciones de los considerandos 26 y 27 de la Directiva muestran cómo quería el legislador que se aplicara la protección de datos». Dictamen 4/2007, p. 5.

10 El GT29 ha sugerido numerosos ejemplos reales de datos generados en el desarrollo de actividades familiares que dejaron de pertenecer a este ámbito cuando se les dio una finalidad distinta. Uno de los ejemplos más significativos es el dibujo realizado por una niña (de su propia familia)

2. Delimitación de actividad exclusivamente personal o doméstica

La excepción doméstica ya estaba recogida en la hoy derogada Directiva 95/46/CE, excluyendo *excepcionalmente* de su ámbito de aplicación, entre otros supuestos, el tratamiento «efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas» (art. 3.2). Matizaba la excepción con ejemplos recogidos en su Considerando 12: «la correspondencia y la llevanza de un repertorio de direcciones». La única diferencia respecto al RGPD es que éste ha añadido nuevos matices en su Considerando 18, fruto de la evolución de los medios tecnológicos y de la experiencia acumulada durante los años transcurridos. Así, se puede leer en el citado Considerando que la «actividad personal o doméstica» resulta incompatible con cualquier «actividad profesional o comercial», incluyendo también una alusión a las actividades personales en el campo de las redes sociales y en línea[11].

Por lo que se refiere al artículo 2.2 RGPD, sigue apareciendo como nota esencial el criterio de *exclusividad* del objeto exceptuado, lo que descarta la aplicación de la excepción a los ficheros mixtos, es decir, a aquellos que sean utilizados simultáneamente en una actividad personal y otra no personal (profesional, comercial, política, etc.). Así, pues, un directorio telefónico, personal o familiar, utilizado posteriormente en una actividad comercial, quedaría automáticamente sometido a las exigencias establecidas en el RGPD.

Más difícil de acotar resulta la expresión «actividad exclusivamente personal o doméstica», que ha requerido precisiones de los tribunales para fijar sus contornos y alcance, precisiones que continúan siendo plenamente válidas

---

aportado más tarde a un procedimiento judicial sobre su custodia: «El dibujo proporciona información sobre el estado de ánimo de la niña y sus sentimientos con respecto a los diferentes miembros de su familia. Como tal, podría entrar en la categoría de *datos personales*. En efecto, el dibujo revela información relativa a la niña (su estado de salud desde un punto de vista psiquiátrico) así como a, por ejemplo, los comportamientos de su padre y de su madre». Dictamen 4/2007, p. 9.

11 Considerando 18 RGPD: «El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas».

con la nueva regulación[12]. En este terreno debemos destacar, por su especial relevancia, la sentencia de la Audiencia Nacional de junio de 2006 sobre la legalidad del tratamiento y cesión de datos con motivo del acto de celebración de las bodas de plata de una de las promociones de la Academia militar de Zaragoza[13].

La Comisión de celebración del evento, integrada por varios miembros de la promoción, había elaborado –a partir de guías de telecomunicaciones y agendas particulares– un listado que recogía los nombres y direcciones de los compañeros, así como el cuerpo al que pertenecía cada uno. Con la única finalidad de contactar con ellos para informarles sobre los actos y organizar la celebración, se entregó el listado a una agencia, que se comprometió a destruirlo o devolverlo al finalizar su cometido. Los hechos fueron objeto de sanción por parte de la AEPD al entender que había existido una cesión no consentida de datos de carácter personal al salir el fichero de la esfera *exclusivamente* personal o doméstica[14]. Sin embargo, la Audiencia Nacional anuló la sanción al considerar lo contrario, ofreciendo las claves para su delimitación.

La Sala no ponía en duda que se había producido un tratamiento de datos en la elaboración del listado, pero advertía que no bastaba con ello para que a tal actividad le fuera aplicable el régimen de protección de la LOPD, pues reconocía a los particulares la facultad de elaborar listados de amistades en sus ordenadores o agendas -electrónicas o manuales- sin necesidad de cumplir las exigencias establecidas en la ley. «Lo relevante para la sujeción al régimen de protección de datos no será por tanto que haya existido tratamiento, sino si dicho tratamiento se ha desarrollado en un ámbito o finalidad que no sea exclusivamente personal o doméstico»[15].

---

12 Al igual que a nivel europeo han sido de gran ayuda y utilidad las orientaciones y aclaraciones contenidas en los Dictámenes del GT29, también lo han sido a nivel nacional los informes y las resoluciones de la AEPD. Los informes recogen las respuestas del gabinete Jurídico de la AEPD a las consultas elevadas en relación a cuestiones controvertidas o novedosas; no tienen carácter vinculante, pero ofrecen luces sobre los posibles pronunciamientos de la AEPD ante las denuncias que se le planteen, por lo que sus orientaciones son muy valiosas.

13 Sentencia 3077/2006 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 15 de junio de 2006 (ECLI: ES:AN:2006:3077).

14 Resolución de la AEPD de 28 de abril de 2004 (R/00260/2004).

15 SAN 3077/2006, cit., FD 3.º Antes de acotar lo que debía entenderse por ámbito exclusivamente personal o doméstico, la Sala procedió a una aclaración interpretativa: el calificativo *personal* no debía ser entendido como realización *individual* del fichero. Los ficheros no dejan de ser personales aunque hayan participado varias personas en su elaboración, siempre que «su finalidad no trascienda de su esfera más íntima o familiar, como la elaboración de un fichero por varios

El punto de partida debía ser, por tanto, la delimitación de los contornos de la actividad *exclusivamente personal o doméstica*, y la apreciación de la Sala fue que una actividad «será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos»[16]. El supuesto enjuiciado cumplía perfectamente con estos requisitos, «pues tiene por objeto mantener los lazos de amistad y compañerismo creados durante el periodo formativo mediante la celebración de un acto puntual de confraternización de todos los miembros de una determinada promoción con ocasión del veinticinco aniversario de su jura de bandera. No se pretende pues una finalidad profesional, aunque todos los partícipes de la celebración pertenezcan a una corporación profesional como es la militar»[17]. Destacaba la sentencia que este tipo de celebraciones, que pueden ser habituales entre universitarios, opositores, familiares, etc., y en las que participa un elevado número de personas, nunca sobrepasa el ámbito privado. «La pretensión de que tales actividades, en cuanto al tratamiento de datos, debieran quedar sujetas a los principios de protección contemplados en la Ley 15/1999, con fundamento en una *concepción maximalista* del principio del consentimiento, como parece expresar la Agencia de Protección de Datos, conllevaría una *desnaturalización de las relaciones sociales*, sometiéndolas a unos *rigores formales* en cuanto al manejo de datos personales totalmente ajenos al sentir social y en modo alguno exigidas por el derecho fundamental a la autodeterminación informativa, *derecho que no es absoluto* y que debe ser interpretado en cuanto a sus manifestaciones y exigencias partiendo de su contraposición con otros derechos y valores constitucionales»[18].

Esta doctrina continúa siendo perfectamente válida con la entrada en vigor del RGPD y de la nueva LOPD, por lo que los tratamientos de datos realizados en el curso de actividades exclusivamente personales y domésticas quedan fuera del ámbito de aplicación de ambas normas.

---

miembros de una familia a los efectos de poder cursar invitaciones de boda». En el supuesto que nos ocupa, por tanto, el hecho de que participaran en la elaboración del fichero todos los integrantes de la Comisión no impediría la aplicación del artículo citado.

16 *Ibid*. Ha sido el criterio utilizado por la AEPD desde entonces, como se puede apreciar, por ejemplo, en su Resolución de 3 de junio de 2015 (Expediente nº E/05493/2014) en la que se refiere a la exclusión de la agenda personal.

17 *Ibidem*.

18 *Ibid*. Las cursivas son nuestras.

Pero, entonces, ¿se prevé alguna protección para los datos generados en las esferas personal y doméstica? La pregunta no es retórica, como prueba el hecho de que la AEPD archivara expedientes de denuncias que, al concernir a tratamientos realizados en el desarrollo de actividades exclusivamente personales o domésticas, los consideraba excluidos del ámbito de aplicación de la normativa de protección. La cuestión fue clarificada por la Audiencia Nacional en 2013 al resolver un recurso contra otra resolución de la AEPD que, precisamente, desestimaba incoar expediente inspector al estimar que el tratamiento denunciado correspondía a una actividad personal. Para la Audiencia, sin embargo, tal decisión no se ajustaba a Derecho, pues los datos obtenidos en el curso de actividades personales o domésticas también son objeto de protección por la normativa, aunque desde una perspectiva distinta[19]. Los hechos que motivaron esta aclaración podríamos resumirlos del modo siguiente. El director de un colegio había solicitado a un alumno de doce años el acceso a los contenidos de su móvil (fotografías, vídeos e historial de navegación) tras la denuncia efectuada por una compañera a la que había mostrado vídeos de contenido pornográfico. El menor accedió a la inspección del director, de la que derivó un expediente disciplinario; los padres del alumno presentaron reclamación ante la AEPD por tratarse de un acceso mediante consentimiento inválido al tratarse de un menor. La AEPD, sin embargo, resolvió archivar la reclamación al estimar que, por un lado, existía base legal habilitante para la actuación del director del centro educativo (un interés legítimo en preservar la integridad moral de los alumnos) y, por otro lado, que los datos personales almacenados en el móvil (el historial de navegación y de descargas de vídeos) se habían originado en el desarrollo de actividades exclusivamente personales, lo que excluía los hechos del ámbito de aplicación de la

19 Sentencia 3877/2013 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 26 de septiembre de 2013 (ECLI: ES:AN:2013:3877). Sobre esta cuestión ya se había pronunciado el GT29 al afirmar que, aunque exista una excepción o el dato tratado no encaje en el concepto de dato personal, «ello no significa que las personas puedan quedar totalmente desprotegidas en esos casos. (...) En aquellos casos en que las normas de protección de datos no se apliquen, determinadas actividades pueden, no obstante, infringir el artículo 8 del Convenio Europeo de Derechos Humanos y Libertades Fundamentales, que protege el derecho a la vida privada y familiar, de acuerdo con la jurisprudencia de mayor alcance del Tribunal Europeo de Derechos Humanos. (...) El ámbito de aplicación de las normas de protección de datos no debe llevarse a su extremo, pero también debe evitarse una limitación indebida del concepto de datos personales. La Directiva ha definido su ámbito de aplicación, excluyendo diversas actividades, y permite cierta flexibilidad al aplicar las normas a las actividades que entran en su ámbito de aplicación» (Dictamen 4/2007, p. 27), pero nunca hasta el extremo de dejar desprotegida la intimidad personal y familiar.

LOPD. Y esta segunda razón fue la que rechazó la Sala, entendiendo que tales datos también están protegidos por las normas de protección de datos[20].

A juicio de la Sala, el artículo 2.2.a) LOPD excluye del ámbito de aplicación de la ley el tratamiento de datos de terceros en actividades personales o domésticas por la mínima capacidad de afectación a la privacidad de los terceros, como puede ser una lista de contactos, pero de ahí no se puede concluir «que quede libre y exento de protección el acceso [inconsentido] a los datos contenidos en un terminal telefónico, a los que bien puede alcanzar la más estricta privacidad»[21]. El historial de navegación y de descargas de vídeos, datos resultantes de la actividad personal del menor, ofrecen claramente información sobre la persona que ha realizado tal actividad, por lo que resultan a todas luces datos protegidos por la ley. Partiendo desde estas premisas, la Sala disiente de la conclusión de la AEPD porque «sentado, pues, que el régimen protector de la Ley Orgánica 15/1999, de 13 diciembre, de Datos de Carácter Personal, es aplicable a las informaciones que se contengan en teléfonos móviles de uso particular –de manera que no les resulta aplicable la exclusión legal de los archivos de naturaleza personal o doméstica–, y partiendo también de que las informaciones a las que se accedió, por parte del personal del centro educativo (vídeos de contenido sexual y trazas de las navegaciones web realizadas), eran susceptibles de calificación como *datos de carácter personal*, se impone ya resolver sobre la licitud o ilicitud de las acciones denunciadas»[22].

En el caso que nos ocupa, entiendo que la Sala y la AEPD deberían haber distinguido entre las dos actividades desarrolladas, que son de distinta naturaleza. La primera es la de navegación del menor, que es exclusivamente personal y está excluida del ámbito de aplicación de la LOPD y cuyo resultado (historial de navegación y de descargas) se convierte en un dato personal protegido por la ley. La segunda en cambio, la actividad del director, no es personal, sino profesional, pues ha sido realizada en el ejercicio de sus atribuciones de dirección, necesitando, por tanto, el consentimiento de los padres del afectado para

---

20 «No comparte el Tribunal las tesis de la Agencia demandada, en el sentido de que los datos contenidos en un teléfono móvil de uso personal queden excluidos de la protección de la Ley Orgánica 15/1999, de 13 diciembre, por tener un contenido estrictamente personal o doméstico». SAN 3877/2013, cit., FD 4º.

21 «Nótese que tales dispositivos pueden albergar determinadas informaciones como las referentes a la salud o la vida sexual, que son objeto de protección reforzada en el art. 7 de la Ley Orgánica 15/1999, de 13 diciembre. Y sin embargo, paradójicamente, quedarían exentos de protección si el acceso a esta clase de terminales fuera libre por no quedar sujetos al régimen protector de la Ley». *Ibid*.

22 *Ibidem*.

acceder a los datos del menor[23] o que exista –como era el caso– una base legal habilitante para proceder legítimamente a la inspección[24].

La propia Audiencia Nacional ha declarado en otras ocasiones que, mediando una relación profesional, la actividad no puede ser considerada de naturaleza personal o doméstica[25], aunque también ha admitido que los datos personales obtenidos de forma legal (con consentimiento) en una relación profesional pueden ser utilizados sin problemas posteriormente en una actividad exclusivamente personal. Es el caso, por ejemplo, del trabajador que obtuvo lícitamente las direcciones electrónicas profesionales de sus compañeros mientras compartió trabajo con ellos en la misma empresa y que utilizó posteriormente para enviarles mensajes de carácter personal[26].

3. Supuestos conflictivos

Los numerosos beneficios para la sociedad, las comunicaciones, la industria, el comercio, etc., de los avances tecnológicos han venido acompañados, como contrapartida, de un riesgo añadido para la intimidad personal y la privacidad cuando éstos se utilizan indebidamente. Veamos algunos supuestos.

---

23 Al tratarse de un menor, deben extremarse las garantías en la obtención del consentimiento. Cfr. GT29, Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), WP 160, adoptado el 11 de febrero de 2009, p. 9.

24 En este caso, la Sala resolvió correctamente –a mi juicio– al considerar que existía base legal habilitante para la inspección del director, que perseguía con su actividad la protección de la compañera que había visualizado los vídeos y la protección del resto de los alumnos.

25 «El tratamiento de imágenes, y los ficheros resultantes, en un ámbito doméstico está excluido del ámbito de aplicación de la LOPD (así lo dispone el artículo 2.2.a de dicha norma) pero quedan comprendidos en la misma aquellos tratamientos que incorporen imágenes de una persona a ficheros como consecuencia de una actividad profesional, como es el caso que nos ocupa, en el que el recurrente en su condición de titular de establecimiento fotográfico capta imágenes de terceros en el ámbito de una relación comercial o profesional, imágenes que sin duda incorporan un elemento artístico y técnico pero que se integran en una relación comercial profesional con ánimo lucrativo». Sentencia 2447/2012 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 18 de mayo de 2012 (ECLI: ES:AN:2012:2447), FD 4º.

26 «Esta Sala considera que el uso que el denunciado hizo de las direcciones de correo electrónico de los ahora actores, a fin de enviarles publicidad de una página web de su titularidad (en la que criticaba a la empresa en la que todos trabajaban) constituye un uso personal de dichos datos (las direcciones de correo) de los mismos, que por tanto ha de ser excluido del ámbito de protección de la Ley Orgánica de Protección de Datos». Sentencia 5441/2012 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 13 de diciembre de 2012 (ECLI: ES:AN:2012:5441), FD 4º.

3.1. *Difusión de datos en Internet: webs, redes sociales, blogs, chats, etc.*

La primera sentencia de relevancia en relación a las actividades en línea fue dictada por el TJCE en noviembre de 2003, pronunciándose sobre la calificación de la difusión sin consentimiento previo de datos personales de terceros a través de una web[27]. B. Lindqvist impartía catequesis junto a otras personas en una parroquia sueca y quiso hacer más asequible la información a los participantes, razón por la que creó una web abierta y sin restricciones de acceso. Recogía en ella, en tono desenfadado, nombres, números telefónicos, aficiones y otros datos del resto de los catequistas, sin haber solicitado previamente su consentimiento. Cuando éstos mostraron su disconformidad con los contenidos eliminó la web, pero el ministerio fiscal inició acciones penales por infracción de la ley sueca de protección de datos, siendo condenada al pago de una multa por haber realizado un tratamiento automatizado de datos personales sin comunicación escrita previa a la Datainspektion, por la inclusión no autorizada de datos personales relativos a la salud de un tercero y por la transferencia no autorizada de datos de carácter personal a países terceros.

La sanción fue recurrida ante el Göta hovrätt, que decidió plantear cuestiones prejudiciales al TJCE, de las que nos interesan dos de ellas: a) si la inclusión de datos personales en una web debía ser considerada tratamiento automatizado; y b) si la actividad de la demandada debía entenderse amparada por la excepción del artículo 3.2., guion 2º, de la Directiva 95/46/CE, es decir, como tratamiento efectuado por «persona física en el ejercicio de actividades exclusivamente personales o domésticas».

Los Gobiernos neerlandés y sueco, personados en el proceso, alegaron que toda difusión de datos personales en una web debía tener la consideración de «tratamiento de datos» y que no cabía calificarla como actividad exclusivamente personal o doméstica. La Comisión europea, además de destacar la accesibilidad universal a los datos difundidos en la web mediante motores de búsqueda, entendía que la excepción contemplada en la Directiva debía quedar reservada únicamente para los casos en los que los datos correspondieran al autor del tratamiento, nunca a terceros. Por su parte, el Abogado General coincidía, en su escrito de conclusiones, en gran medida con las alegaciones

---

[27] STJCE de 6 de noviembre de 2003, asunto C-101/01. Petición de decisión prejudicial planteada por el Göta hovrätt (Suecia): Bodil Lindqvist (ECLI:EU:C:2003:596).

citadas[28]. Entendía que las actividades personales y domésticas debían quedar referidas únicamente a las «actividades claramente privadas y reservadas, destinadas a quedar confinadas en la esfera personal o doméstica de los interesados. No creo, por tanto, que pueda considerarse como tal una actividad que presenta una marcada connotación social, como la actividad de catequesis desarrollada por la señora Lindqvist en el seno de la comunidad parroquial. Y mucho más si se considera que el tratamiento efectuado por la señora Lindqvist trasciende su esfera personal o doméstica, y supone, además, la divulgación de datos personales en una página web accesible a cualquiera, desde cualquier parte del mundo»[29].

El TJCE declaró en su sentencia que: a) «La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un *tratamiento total o parcialmente automatizado de datos personales* en el sentido del artículo 3, apartado 1, de la Directiva 95/46»[30]; b) el tratamiento descrito no encaja en la excepción de actividades exclusivamente personales o domésticas, pues tal excepción «contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente no es éste el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas»[31].

Éste ha sido el criterio aplicado desde entonces por los tribunales nacionales y por la AEPD. Una web o un blog sin limitación de acceso exceden el ámbito doméstico, por lo que, en principio, los datos de carácter personal de terceros que se difundan a través de ella quedaban protegidos por la antigua Directiva y ahora por el RGPD. Hemos afirmado que los datos personales *en principio* quedan protegidos de su difusión inconsentida, pero no siempre, pues puede prevalecer el derecho a la información (cuando se trata de unos hechos de interés general) o el ejercicio de la libertad de expresión y opinión. En el primer supuesto, los tribunales exigen para su licitud que los datos personales difundidos sean mínimos (como puede ser el nombre y apellidos) y obtenidos

---

28 Acertadamente se distanció de la interpretación de la Comisión que pretendía excluir de la excepción el tratamiento de los datos de terceros. Lo que se recoge en un directorio postal personal son datos de terceros y, sin embargo, pueden ser tratados para actividades personales sin problema alguno. Con su interpretación, la Comisión confundía vida privada con intimidad.

29 Escrito de conclusiones del Abogado General dentro del proceso seguido en el asunto C-101/01 (ECLI:EU:C:2002:513), n. 34.

30 STJCE citada, n. 27.

31 STJCE citada, n. 47.

de un modo legal[32]. En el segundo supuesto, cuando se trata de una opinión –no información– vertida en una web o en un blog, no resulta de aplicación la normativa de protección de datos personales más que para solicitar la cancelación del comentario u opinión y buscar el amparo legal a través de la protección del honor y buena fama si se consideran lesionados[33].

Especial atención merecen las fotografías o vídeos de contexto familiar o de amistad realizados en un espacio público en los que también aparecen de modo accesorio terceros identificados o identificables. Si las imágenes no son difundidas fuera del ámbito familiar no revisten problema alguno porque la incidencia sobre la privacidad de los afectados es mínima o nula. Sin embargo, es frecuente que las fotografías o vídeos sean puestos a disposición del público en general a través de Internet (en una web o en una plataforma). En estos supuestos, el tratamiento no estaría excluido de la aplicación de las normas de protección de datos, lo que supondría la obligación de recabar el consentimiento explícito de los terceros afectados[34] o, como mínimo, prever un fácil ejercicio del derecho de rectificación/cancelación por esos terceros[35].

---

32 Cfr. Sentencia 1960/2013 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 10 de mayo de 2013 (ECLI: ES:AN:2013:1960). Se pronuncia sobre la inclusión de los nombres de personas condenadas por acoso laboral aprovechando la difusión de la noticia en la web de un periódico. Los nombres habían sido incluidos en los comentarios de los lectores a la noticia publicada. Este criterio es aplicado también en las redes sociales cuando el acceso a los contenidos sea universal. Cfr. Sentencia 594/2017 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 14 de febrero de 2017 (ECLI: ES:AN:2017:594). Se refiere a una noticia colgada en el muro de Facebook en la que aparecían nombre y apellido de personas sancionas tras una inspección de trabajo.

33 La AEPD, aplicando la doctrina de la SAN 1960/2013 citada, resuelve las denuncias de este tipo indicando a quienes las presentan que deben ejercitar su derecho de rectificación/cancelación de la entrada del blog que consideran ilegal, y acudir a los tribunales si consideran su contenido constitutivo de delito. Cfr. Resolución R/01257/2017 de 17 de julio de 2017 (Expediente nº TD/00489/2017) y Resolución R/01978/2017 de 17 de julio de 2017 (Expediente nº TD/00904/2017). Los recursos presentados contra estas resoluciones fueron desestimados por la AEPD, que se reafirmó en sus argumentaciones. Cfr. Resolución de Recurso de Reposición nº RR/00624/2017, de 13 de septiembre de 2017, y Resolución de Recurso de Reposición nº RR/00622/2017, de 13 de septiembre de 2017.

34 Cfr. Sentencia 131/2018 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 23 de enero de 2018 (ECLI: ES:AN:2018:131). Inadmite el recurso contra resolución de la AEPD de 27 de noviembre de 2015 sobre una fotografía colgada en la web de SEAT tomada en un estadio de futbol; se habían tomado todas las precauciones legales antes de su difusión.

35 Cfr. Rallo, A.; Martínez, R., «Protección de datos personales y redes sociales: obligaciones para los medios de comunicación», *Quaderns del CAC* 37, XIV (2) (2011), pp. 44 y 47. Exponen estos autores que este es el planteamiento de la AEPD, «priorizar el ejercicio de derechos de cancelación como método para la resolución de conflictos reservando el aparato sancionador para los supuestos más graves».

Junto al tratamiento de datos personales en webs o blogs de acceso universal, también ha suscitado numerosas controversias la difusión de datos personales en las redes sociales[36]. La principal diferencia frente a una web es que la red social ofrece al usuario la posibilidad de restringir a una lista limitada de contactos el acceso a los contenidos o permitir el acceso a todos los usuarios de la red (en este caso se aplicaría lo ya expuesto sobre las webs). El GT29 se pronunció al respecto en su Dictamen 5/2009 sobre las redes sociales en línea[37], en el que define la red social como un servicio de la Sociedad de la Información (SRS) que, en primer lugar, exige a los usuarios la consignación de sus propios datos personales para generar su perfil y, además, proporciona herramientas para compartir en línea otros contenidos propios (fotografías, crónicas, comentarios, música, vídeos o enlaces hacia otros sitios) y para contactar e interactuar con otros usuarios[38]. Según la normativa, los proveedores de SRS son los responsables del tratamiento, quedando al margen los usuarios de la red social, pero «en algunos casos, la exención doméstica puede no cubrir las actividades de un usuario de SRS y puede entonces considerarse que el usuario ha asumido algunas de las responsabilidades de un responsable de datos»[39].

El GT29 especifica en el Dictamen 5/2009 algunos de los supuestos en los que la actividad del usuario deja de ser exclusivamente personal o doméstica y requiere el consentimiento de los terceros afectados para la difusión de sus datos[40]. Estos supuestos se producen, en primer lugar, «cuando el SRS se utiliza como una plataforma de colaboración para una asociación o una empresa. Si un usuario de SRS actúa en nombre de una empresa o de una asociación o utiliza el SRS principalmente como una plataforma con fines comerciales, políticos o sociales, la exención no se aplica. En este caso, el usuario asume la plena responsabilidad de un responsable del tratamiento de datos que revela datos personales a otro responsable del tratamiento de datos (SRS) y a terceros (otros usuarios de SRS o incluso, potencialmente, a otros responsables del

---

36 Además del citado artículo de RALLO y MARTÍNEZ, pp. 41-51, *vid*. TRONCOSO REIGADA, A., «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales» (Parte una), *IDP Revista de Internet, Derecho y Política* (UOC), 15 (2012), pp. 61-75.

37 GT29, Dictamen 5/2009 sobre las redes sociales en línea, WP 163, adoptado el 12 de junio de 2009. La AEPD, en su Informe 0197/2013, recogió prácticamente todo el contenido de este Dictamen.

38 Dictamen 5/2009, p. 5.

39 Dictamen 5/2009, p. 6.

40 A estos efectos, es irrelevante que los terceros afectados pertenezcan o no a la misma red social. Dictamen 5/2009, pp. 9 y 12.

tratamiento de datos que tienen acceso a ellos)»[41]. En segundo lugar, tampoco se podría acoger a la excepción doméstica la actividad del usuario que no limita su lista de contactos al ámbito familiar o de amistad, abriendo el acceso a su perfil y contenidos a personas completamente desconocidas[42]: «cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, cuando todos los miembros que pertenecen al SRS pueden acceder a un perfil o cuando los datos son indexables por los motores de búsqueda, el acceso sobrepasa el ámbito personal o doméstico. Del mismo modo, si un usuario decide, con perfecto conocimiento de causa, ampliar el acceso más allá de los *amigos* elegidos, asume las responsabilidades de un responsable del tratamiento de datos»[43]. Y, por último, tampoco se podría acoger a la excepción de actividad doméstica el usuario que, habiendo limitado su lista de contactos (y, por tanto, el acceso) al círculo estrictamente familiar o de amistad, incluya entre sus contenidos datos personales de carácter sensible de alguno de ellos o de terceros[44].

La Audiencia Nacional ha tenido la oportunidad de pronunciarse en diversas ocasiones sobre la cesión inconsentida de datos personales en las redes sociales, en algunas de ellas concurriendo circunstancias agravantes por

---

41 «En tales circunstancias, el usuario necesita el consentimiento de las personas interesadas u otra base legítima que figure en la Directiva [ahora en el RGPD] relativa a la protección de datos». Dictamen 5/2009, p. 6.

42 «Generalmente, el acceso a los datos de un usuario (datos del perfil, mensajes, historias...) se limita a los contactos elegidos. Sin embargo, en algunos casos, los usuarios pueden adquirir un gran número de contactos terceros y no conocer a algunos de ellos. Un gran número de contactos puede indicar que no se aplica la excepción doméstica y el usuario podría entonces ser considerado como un responsable del tratamiento de datos». Dictamen 5/2009, p. 6. Para evitar que este acceso ilimitado se produzca de forma involuntaria, el citado Dictamen sugiere (p. 7) que el propio SRS establezca por defecto parámetros de acceso que permitan al usuario ser consciente de sus decisiones en relación a los permisos a terceros, y que adopte medidas para evitar la localización de perfiles mediante motores de búsqueda, ya sean externos o internos del propio SRS. En un Dictamen anterior ya había recomendado extremar las medidas de prudencia cuando se trate de usuarios menores de edad. Cfr. Dictamen 2/2009 sobre la protección de los datos personales de los niños, cit., pp. 10-11.

43 «En la práctica, se aplica entonces el mismo régimen jurídico que cuando una persona utiliza otras plataformas tecnológicas para publicar datos personales en Internet». Dictamen 5/2009, p. 6.

44 Dictamen 5/2009, p. 7. Más adelante añade que «Los datos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia sindical y los datos relativos a la salud y a la vida sexual se consideran sensibles. Los datos personales sensibles sólo pueden publicarse en Internet con el consentimiento explícito de la persona interesada o si esta misma persona ha hecho públicos estos datos». Dictamen 5/2009, p. 8.

tratarse de difusión de imágenes de menores o por afectar a datos sensibles de terceros. En el primer supuesto, se desestimaba la aplicación de la excepción doméstica por tratarse de la difusión de un vídeo en el que aparecían menores de ocho años perfectamente identificables conversando con el titular del perfil durante la visita a un zoo, sin que se hubiera recabado el consentimiento previo de sus padres o tutores para la difusión[45]. En el segundo supuesto se resolvía una cuestión más delicada, pues, mediante perfiles falsos se había difundido en Facebook y Badoo la imagen, nombre y apellidos de una persona a la que se atribuía falsamente una enfermedad con ánimo de provocar su exclusión social[46].

En conclusión, el tratamiento de datos ajenos por un usuario particular en una red social sólo se considera como actividad doméstica y, por tanto, excluida de la aplicación del RGPD y de la LOPD, cuando, sin incluir datos sensibles de terceros, limite razonablemente su lista de contactos al círculo más cercano[47]. No obstante, habrá que analizar y ponderar cada caso concreto, pues ni todas las redes sociales son iguales, ni todas las que más o menos lo son ofrecen los mismos servicios. Por ejemplo, un usuario puede publicar un tweet dirigido a sus seguidores convencido de que sus destinatarios constituyen un grupo restringido, pero la posibilidad ofrecida por la aplicación de *retweetear* ese mismo mensaje hace imposible que le pueda ser aplicada la excepción doméstica. Y tampoco sería aplicable la excepción doméstica cuando se crea un grupo de whatsapp en el que los integrantes superan el círculo cercano del administrador y no existe relación entre ellos, pues los números de móviles suelen llevar asociados los datos de identificación (imagen y nombre) de los titulares de los terminales[48].

---

45 Cfr. Sentencia 215/2013 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 2 de enero de 2013 (ECLI: ES:AN:2013:215). Ya había resuelto la AEPD en el mismo sentido con fecha 7 de octubre de 2011.

46 Cfr. Sentencia 348/2016 de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 2 de febrero de 2016 (ECLI: ES:AN:2016:348). La sentencia no entra en el fondo del asunto, que da a entender que considera delictivo, pues resolvía un recurso por indefensión de la sancionada por la AEPD.

47 Aunque no se trate de una red social, esta consideración es extensible a los tratamientos de datos en una «nube», que pueden restringirse más o menos en función de los deseos del usuario. Cfr. Leenes, R., «¿Quién controla la nube?», *IDP Revista de Internet, Derecho y Política* (UOC), 11 (2010), p. 9.

48 La AEPD sancionó a un Ayuntamiento por crear un grupo de WhatsApp con 255 vecinos para ofrecer información municipal y que no habían prestado consentimiento para tal uso de sus datos. *Vid*. Resolución de la AEPD R/03041/2017, de 20 de noviembre de 2017 (Procedimiento nº AP/00023/2017). En su FD VII (p. 13) afirma: «se recuerda al citado Ayuntamiento la exigencia de contar no sólo con el consentimiento previo e inequívoco los titulares afectados para incluir sus datos de carácter personal en grupos de WhatsApp, o de cualquier otra aplicación de

3.2. *Datos obtenidos mediante videovigilancia en el ámbito doméstico*

La videovigilancia efectuada por un particular por motivos de seguridad del domicilio privado o de su entrada sin captar imágenes de la vía pública o de los espacios compartidos con otros vecinos encajaría perfectamente en la excepción de actividades exclusivamente personales o domésticas[49]. Los problemas se plantean cuando: a) la videovigilancia ha sido contratada con una empresa especializada (con conexión a centro de alarma); b) el sistema de videovigilancia pertenece a una comunidad de propietarios y afecta, por tanto, a espacios compartidos por los diversos vecinos que integran la comunidad; c) los dispositivos de videovigilancia captan una parte de la vía pública.

Los dos primeros supuestos no quedan amparados por la excepción doméstica, pero el tercero sí puede estarlo según las circunstancias concretas. El primer supuesto (videovigilancia contratada) no resulta amparado por la excepción porque el tratamiento, aun realizándose en el ámbito doméstico, no es efectuado por una persona física y, además, implica la intervención de un tercero (empresa) extraño a ese ámbito, regulándose, lógicamente, por otras normas específicas para garantizar los derechos del contratante. El segundo tampoco encaja en la excepción porque la captación y tratamiento de datos (imágenes de personas identificables[50]) se realiza en un ámbito que, siendo privado, no es estrictamente doméstico y se presupone que su finalidad, además

---

mensajería instantánea que ofrezca un servicio de comunicación electrónica grupal semejante, sino también de que dicho uso de datos personales responda a las finalidades concretas para las cuales se obtuvieron y fue autorizado su tratamiento por sus titulares». La AEPD sólo sancionó por un uso que no se correspondía con la finalidad con la que habían sido cedidos los datos, pero podría haber sancionado también por la cesión de los datos reflejados en cada contacto, que, como hemos afirmado en el texto suelen contener una imagen, un nombre, un estado, etc., fácilmente asequibles para todos los componentes del grupo.

49 A diferencia del RGPD, la nueva LOPD dedica el artículo 22 a regular explícitamente esta cuestión, aunque el alcance jurídico es el mismo.

50 Aclara el GT29 en su Dictamen 4/2007 que «de modo general, se puede considerar *identificada* a una persona física cuando, dentro de un grupo de personas, se la *distingue* de todos los demás miembros del grupo. Por consiguiente, la persona física es *identificable* cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo *ble*)» (p. 13), pero, también aclara que «la mera e hipotética posibilidad de singularizar a un individuo no es suficiente para considerar a la persona como *identificable*. Si, teniendo en cuenta *el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona*, no existe esa posibilidad o es insignificante, la persona no debe ser considerada como *identificable* y la información no debe catalogarse como *datos personales*» (p. 16). Sería el caso, por ejemplo, de las cámaras de baja calidad que no permiten reconocer los rostros de las personas captadas, sino solamente su presencia.

de la seguridad, es la de identificar a las personas que entren en su radio de captación[51]. No quiere esto decir que no se puedan llevar a cabo estos tratamientos, sino que quedarían dentro del ámbito de aplicación del RGPD y de la LOPD, debiendo cumplir los requisitos generales establecidos para cualquier otro tratamiento. En cuanto al tercer supuesto, que implica la captación de una parte de la vía pública, dependerá del tipo de dispositivo utilizado, de las alternativas posibles y de la proporcionalidad de la medida.

La cuestión preocupó desde un principio al GT29, que adoptó ya en el año 2004 un primer Dictamen[52] con análisis de la situación y las recomendaciones oportunas. Sin embargo, a pesar de su intención de ofrecer criterios claros, sólo ofreció alguna luz al respecto, pero no toda la claridad deseada. Del Dictamen se extrae como conclusión que una persona física podría instalar un sistema de videovigilancia para garantizar la seguridad de su domicilio incluso captando parte de la vía púbica, siempre que se respeten los derechos e intereses legítimos de los vecinos y de los transeúntes[53]. Por esta razón afirma que «deberá prestarse especial atención a la orientación del equipo de vídeo, a la obligación de enviar avisos e información y al borrado oportuno de las imágenes (en el plazo de unas horas) si no se ha producido allanamiento de morada ni otros delitos»[54].

---

51 «En estos casos, en los que la finalidad del tratamiento implica la identificación de personas, puede asumirse que el responsable del tratamiento o cualquier otra persona implicada tiene o puede tener medios que «puedan ser razonablemente utilizados», para identificar al interesado. De hecho, sostener que las personas físicas no son identificables, cuando la finalidad del tratamiento es precisamente identificarlos, sería una contradicción flagrante (...) Como la finalidad de la videovigilancia es, sin embargo, identificar a las personas que aparecen en las imágenes de vídeo en todos aquellos casos en los que esa identificación es considerada necesaria por el responsable del tratamiento, hay que considerar el uso del sistema en sí como tratamiento de datos sobre personas identificables, aun cuando algunas de las personas filmadas no sean identificables en la práctica». GT29, Dictamen 4/2007, pp. 17-18. Se trataría de una presunción que admite prueba en contrario.

52 Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, WP 89, adoptado el 11 de febrero de 2004. El GT29 manifestaba desde un principio la necesidad de elaborar unos criterios claros al respecto por la repercusión que la captación y/o grabación de imágenes podría tener sobre las personas (condicionamiento psicológico excesivo), afectando al derecho a la privacidad y a la libre circulación. Dictamen citado, p. 6.

53 El propio Dictamen afirma que «estos derechos e intereses están protegidos, independientemente de los principios de la protección de datos, por las disposiciones generales (código civil) que protegen los derechos, la imagen, la vida familiar y el ámbito privado de las personas (pensemos, por ejemplo, en el ángulo visual de una cámara instalada en el exterior de un apartamento, lo que permite grabar, sistemáticamente, a los clientes de una clínica o un bufete de abogados situados en el mismo piso y, de este modo, inmiscuirse de manera ilegal en el secreto profesional)». Dictamen 4/2004, p. 14.

54 Dictamen 4/2004, pp. 14-15.

Sin embargo, el TJUE fue más tajante en su sentencia de 2014[55] sobre esta cuestión al señalar que la excepción contemplada en el artículo 3.2 de la Directiva 95/46/CE [ahora en el RGPD] no admitía interpretaciones amplias, pues de lo contrario se correría el riesgo de facilitar la vulneración de los derechos fundamentales a la protección de los datos de carácter personal y a la vida privada de terceros. En este asunto se dilucidaba la cuestión prejudicial planteada por el Tribunal Supremo Administrativo de la República Checa sobre si quedaba amparada bajo el paraguas de la excepción doméstica la instalación de un sistema de videovigilancia que no sólo captaba imágenes de la entrada del domicilio particular, sino también una parte de la vía pública, grabando en un disco duro las imágenes de las personas que transitaban por ella.

En su argumentación, el TJUE puso de relieve que la exclusión del ámbito de aplicación de la Directiva en relación a las actividades personales y domésticas debía ser interpretada siempre en sentido estricto, en primer lugar porque las restricciones a las garantías de los derechos fundamentales a la vida privada y a la protección de datos de carácter personal nunca debían sobrepasar los límites de lo estrictamente necesario[56] y, en segundo lugar, porque el propio texto normativo utilizaba el término *exclusivamente* para despejar las dudas que pudieran surgir en torno a la cuestión[57]. El TJUE vino a admitir en su sentencia que si la grabación afectaba únicamente al domicilio particular y se hiciera con la finalidad de proteger los bienes, la salud y la vida de los propietarios, quedaría amparada por la excepción[58], pero si la «vigilancia cubre también el espacio público, no constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas a efectos de la

---

55 STJUE de 11 de diciembre de 2014, asunto C-212/13. Petición de decisión prejudicial planteada por el Nejvyšší správní soud (República Checa): František Ryneš (ECLI:EU:C:2014:2428).

56 Cfr. STJUE citada, nn. 28-29.

57 Cfr. STJUE citada, n. 30: «Tal interpretación estricta se fundamenta también en el propio texto de la disposición que acaba de citarse, según el cual la Directiva 95/46 no se limita a prever que sus disposiciones no se aplicarán al tratamiento de datos personales en el ejercicio de actividades personales o domésticas, sino que exige que se trate del ejercicio de actividades «exclusivamente» personales o domésticas».

58 A este interés legítimo de seguridad se debe el que se puedan captar las imágenes de la entrada al domicilio (sin invadir la vía pública), como se afirma en el n. 34 de la sentencia: «Al mismo tiempo, la aplicación de las disposiciones de dicha Directiva permite, en su caso, tener en cuenta, con arreglo en particular a los arts. 7, letra f), 11, apartado 2, y 13, apartado 1, letras d) y g), los intereses legítimos del responsable del tratamiento de los datos, intereses que consisten concretamente, como en el litigio principal, en proteger los bienes, la salud y la vida de dicho responsable y los de su familia».

citada disposición [Directiva 95/46]»[59]. En definitiva, tal grabación estaría sujeta a todas las exigencias de la citada norma. Como ya hemos afirmado, el TJUE no niega que existan supuestos en los que un interés legítimo habilite a una persona física para captar o grabar imágenes en la vía pública[60], sino que en este supuesto concreto de seguridad del domicilio particular, una vez analizadas las circunstancias y ponderados los intereses y derechos en juego de los afectados, entiende que el interés alegado por el particular (la seguridad personal y de la propiedad) no era suficiente para legitimar el tratamiento de datos obtenidos en el espacio público sin la información y el consentimiento de los afectados.

En el terreno práctico de la videovigilancia, nos ofrece mayor claridad la Instrucción 1/2006, de 8 de noviembre, de la AEPD sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[61]. A ella habría que añadir los recientes informes emitidos por la AEPD en 2018 con motivo de la entrada en vigor del RGPD y las más de cuatrocientas resoluciones adoptadas por la AEPD sobre la materia en los últimos diez años. En estos documentos se advierte con mayor claridad la distinción entre los diversos dispositivos, que a su vez pueden desempeñar diferentes funciones, de lo que dependerá que su utilización esté amparada o no por la excepción de actividades domésticas.

3.2.1. Los videoporteros y mirillas digitales

Como vino a reconocer tempranamente la AEPD en sus resoluciones, los videoporteros quedan excluidos del ámbito de aplicación de la normativa al no ser considerados dispositivos de videovigilancia. La razón es que este tipo

---

59 STJUE citada, n. 35. *Vid*. más extensamente al respecto las conclusiones presentadas por el Abogado General el 10 de julio de 2014, nn. 63-67.

60 Ya se había manifestado en este sentido en su STJUE de 24 de noviembre de 2011, asuntos acumulados C-468/10 y C-469/10. Petición de decisión prejudicial planteada por el Tribunal Supremo (España): ASNEF y FECEMD (ECLI:EU:C:2011:777). Sobre el alcance del interés legítimo como base justificadora del tratamiento, *vid*. GUASCH PORTA, V.; SOLER FUENSANTA, J.R., «El interés legítimo en la protección de datos», *Revista de Derecho UNED*, 16 (2015), pp. 417-438.

61 En España, la excepción doméstica en materia de videovigilancia también fue recogida en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE nº 296, de 12 de diciembre de 2006, pp. 43458-43460). Su artículo 1.3 establece que «no se considera objeto de regulación de esta Instrucción el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar».

de dispositivos sólo muestra la imagen de la persona durante unos segundos (no está activado permanentemente) al ser pulsado y no permite la grabación de imágenes. Las denuncias presentadas se han ido resolviendo con el archivo de las actuaciones, pues «el tratamiento resultante de las imágenes captadas se circunscribe al ejercicio exclusivo de actividades domésticas, cumpliendo los requisitos de finalidad y proporcionalidad exigidos por la actual normativa en materia de protección de datos»[62]. No obstante, en estas primeras resoluciones la AEPD consideraba conveniente, no obligatorio, que se informara a las personas mediante un cartel colocado en la entrada sobre la existencia del dispositivo.

En su Informe 0335/2009, respondiendo a la consulta de un particular, la AEPD realizó una serie de matizaciones ante la variedad de este tipo de dispositivo y su posible incidencia sobre la vía pública, concluyendo que siempre que el videoportero se limitara a las funciones descritas anteriormente (activación por pulsación, escasos segundos y sin grabación de imágenes) se consideraría excluido del ámbito de aplicación de la normativa; pero si el dispositivo permitía la activación sin ser pulsado, o la grabación de imágenes o la visualización en monitores ajenos al dispositivo (monitores, red de televisión, ordenador, etc.), quedaría sometido a las exigencias de las normas de protección de datos[63].

Otro dispositivo, cada vez más utilizado, es la mirilla digital, apta para colocar en sustitución de la tradicional mirilla óptica que suele tener la puerta de los domicilios particulares y que aporta la ventaja de aumentar la imagen del exterior en una pantalla antes de franquear la entrada. La AEPD tampoco considera la función de este dispositivo como videovigilancia y, por tanto, lo

---

62 Resolución de 18 de marzo de 2009 (Expediente nº E/01431/2008), FD III. En este supuesto se resolvía la denuncia formulada contra una residencia de mayores, pero ya se habían resuelto otras similares mediante resoluciones de 1 de septiembre de 2008 (denuncia formulada contra el Pub La Iguana, Expediente nº E/01131/2007) y de 23 de enero de 2009 (denuncia formulada contra el Pub Eddie, Expediente nº E/00884/2008).

63 Es el criterio seguido en sus posteriores resoluciones. Por ejemplo, en su Resolución de 23 de enero de 2017 (Expediente nº E/02806/2016), FD III, afirma: «en aquellos casos en los que la utilización de videoportero se limite a su función de verificar la identidad de la persona que llamó al timbre y a facilitar el acceso a la vivienda, como es el caso que nos ocupa, no será de aplicación la normativa sobre protección de datos. Sin embargo, si el servicio se articula mediante procedimientos que reproducen y/o graban imágenes de modo constante, y resultan accesibles (ya sea a través de Internet o mediante monitores), resultará de plena aplicación la Instrucción 1/2006». *Vid*. en el mismo sentido Resolución de la AEPD de 14 de febrero de 2017 (Expediente nº E/04687/2016).

excluye de la normativa sobre protección de datos «siempre que su función se limite a verificar la identidad de la persona que llamó al timbre y a facilitar el acceso a la vivienda»[64].

El problema con este dispositivo es que algunos modelos permiten su activación sin necesidad de que llamen al timbre y grabar las imágenes que captan del exterior, pudiendo incidir sobre los vecinos e incluso sobre el interior de la vivienda que tenga enfrente cada vez que se abra la puerta de ésta. En estos supuestos se requiere para su utilización, con más razón que para el videoportero exterior, la autorización de la comunidad de propietarios[65], pues, a diferencia de éste, que tan sólo podría incidir sobre el exterior de la vivienda, la mirilla digital sería idónea para grabar en una zona interior común a todos los vecinos[66].

3.2.2. La videovigilancia con cámaras

El uso de cámaras de videovigilancia con fines de seguridad se ha extendido de tal forma en los últimos años que se ha convertido en uno de los objetos de denuncia más recurrente en las reclamaciones formuladas ante la AEPD, lo que ha permitido elaborar unos criterios esclarecedores para resolver las frecuentes controversias.

Uno de los motivos que mueve a los ciudadanos –también a los Cuerpos de Seguridad del Estado– a formular las denuncias contra las cámaras privadas es la sospecha de que captan partes del espacio público o de propiedades colindantes, lo que ocasiona la sensación de pérdida de privacidad y de libertad

---

64 Resolución de la AEPD de 28 de febrero de 2017 (Expediente nº E/04804/2016), FD III.

65 «Cuando la mirilla digital graba imágenes la situación cambia por completo. Al estar grabando imágenes fuera de la propiedad privada del titular de la mirilla, el tratamiento no puede considerarse como desarrollado en el ejercicio de actividades exclusivamente personales o domésticas. Para que el tratamiento se excluya de la LOPD, como tratamiento doméstico, la grabación de imágenes debe circunscribirse únicamente al entorno privado familiar y particular, no puede salir de ese entorno (no puede incluir en la grabación imágenes de fuera, como los elementos comunes del rellano comunitario por donde pasan vecinos, familiares de los vecinos, repartidores, etc. personas ajenas al núcleo estrictamente familiar). Por esta razón cuando se toman imágenes en lugares comunes es necesaria la autorización de la comunidad de propietarios cumpliendo con los requisitos establecidos en la Ley 49/1960, de 21 de julio de Propiedad Horizontal». Resolución de la AEPD R/02373/2017 de 11 de septiembre de 2017 (Procedimiento nº A/00273/2017), FD III.

66 «La diferencia esencial es que los videoporteros están ubicados en el exterior de las casas no en el interior de las mismas (no graban elementos comunes) y su instalación en una comunidad de propietarios necesita de la autorización de la misma por la junta de propietarios». *Ibid*.

de circulación en zonas en las que no debería ser así; es decir, se produce el condicionamiento psicológico excesivo al que alude el GT29 en el ya citado Dictamen 4/2004. Pero, tras la lectura de cientos de resoluciones de la AEPD sobre la instalación de estas cámaras, se advierte también que gran parte de las denuncias responden a una enemistad manifiesta entre denunciado y denunciante, que utiliza este medio como un arma más para importunar a su *enemigo*. Esta es la razón de que numerosas resoluciones de la AEPD finalicen con el archivo de las actuaciones, en unas ocasiones porque se comprueba que las cámaras denunciadas sólo captan la imágenes de la propiedad de quien la instaló y en otras porque se trata de dispositivos que tan sólo simulan ser cámaras de videovigilancia, pero no lo son, o porque, siéndolo, han sido inutilizadas a propósito por su instalador, pretendiendo únicamente disuadir a vecinos o transeúntes de la comisión de actos ilícitos sobre la propiedad aparentemente vigilada.

Las cámaras particulares de vigilancia, con reproducción en tiempo real o con grabación, que captan solamente los espacios privados de quien la instaló quedan excluidas por la excepción doméstica de la aplicación de la normativa de protección de datos[67]. Así lo establece la regulación, aplicada de forma sistemática desde un principio por la AEPD[68], que tan sólo insta a la retirada cuando los dispositivos no son aptos para esta limitación, como pueden ser las cámaras esféricas de 360º, o impone la limitación de la captación de imágenes mediante cintas adhesivas o carcasas que impidan captar imágenes más allá de la propiedad particular que se pretenda vigilar[69]. Cuando se trata de propiedades particulares de uso común, es decir, los espacios comunes en comunidades

---

67 No son sólo los artículos 2.2.c) RGPD y 2.2.a) LOPD los que excluirían esta actividad del ámbito de aplicación de la normativa de protección de datos, sino que además el nuevo artículo 22.5 (videovigilancia) la recoge de modo explícito al establecer que «Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación [del artículo 22] el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio».

68 *Vid*., por ejemplo, Resolución de 23 de enero de 2017 (Expediente nº E/02112/2016), Resolución de 6 de febrero de 2017 (Expediente nº E/03854/2016), Resolución de 13 de febrero de 2017 (Expediente nº E/03148/2016), Resolución de 14 de febrero de 2017 (Expediente nº E/03409/2016), Resolución de 22 de febrero de 2017 (Expediente nº E/03400/2016), Resolución de 14 de marzo de 2017 (Expediente nº E/03146/2016), Resolución de 12 de mayo de 2017 (Expediente nº E/04711/2016), etc.

69 Sobre las cámaras esféricas, *vid*. Resolución de 27 de marzo de 2017 (Expediente nº E/03319/2016). Sobre la limitación de los dispositivos para que sólo capten la propiedad particular, *vid*. Resolución de 20 de febrero de 2018 (Expediente nº E/05394/2017).

de propietarios, no cabe la consideración de tratamiento doméstico, por lo que se requerirá la autorización de la junta de propietarios para su instalación, además de cumplir con los requisitos de información, posibilidad de cancelación, etc., establecidos por la ley[70].

Situación distinta es la derivada de la videovigilancia de una propiedad particular que, para poder ser llevada a cabo con eficacia, precisa captar incidentalmente parte de la vía pública o de propiedades colindantes. Es el supuesto que la AEPD describe del siguiente modo: «en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas. A veces, también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta»[71]. En estos supuestos será necesario para su licitud que sólo se capte lo imprescindible de la vía pública, que no exista una alternativa menos invasiva y que haya proporcionalidad entre el fin perseguido y el sacrificio de los bienes afectados[72]. La propia

---

70 Los espacios que pertenecen a la comunidad de propietarios no pueden acogerse a la excepción de tratamiento doméstico, aunque sean de uso privativo por alguno de los vecinos. Sin embargo, en algún caso aislado, dadas las dificultades –por enemistad manifiesta– para obtener la autorización de la junta de propietarios para instalar cámaras de videovigilancia en este tipo de espacios siendo necesarias por seguridad, la AEPD ha entendido que se pueden instalar acogiéndose a un interés legítimo [recogido ahora en el artículo 6.1.f) RGPD] que no perjudique los derechos fundamentales del resto de vecinos. *Vid*. Resolución de 15 de noviembre de 2017 (Expediente nº A/00373/2017). En este supuesto se trataba de una terraza a la que sólo tenía acceso una vecina a través de su vivienda, por lo que no se perjudicaba a nadie si la vigilancia se limitaba estrictamente a la terraza. Distinta sería su instalación para vigilar una plaza de garaje, que, al ser accesible a todos los vecinos, no podría estar legitimada por el RGPD, como ha puesto de relieve la AEPD en un informe de 2018. Cfr. https://www.aepd.es/media/informes/informe-juridico-rgpd-camaras-plaza-garaje.pdf [consulta: 31-05-2018].

71 Resolución de 11 de enero de 2018 (Expediente nº E/03264/2017), FD IV (p. 4). A estos supuestos ya se refería la Instrucción 1/2006 en su artículo 4.3 al disponer que «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».

72 «En este sentido, la posibilidad de captar un pequeño ángulo de la vía pública a través de una cámara de vigilancia, ésta deberá de cumplir el principio de proporcionalidad, sin que sea posible extender la grabación de imágenes a un alcance mayor al que resulte necesario para garantizar la seguridad de las instalaciones. Por ello, la referencia a los alrededores de las instalaciones, únicamente resultaría ajustada a la normativa de protección de datos en caso de que la misma se refiera exclusivamente a aquellos espacios públicos sin cuya grabación resultaría en todo punto imposible el control de la seguridad en el acceso a las instalaciones, sin que en modo alguno esta

AEPD pone de relieve que de ningún modo se puede entender esta excepción como «una habilitación para captar imágenes en espacios públicos, puesto que en ningún caso puede admitirse el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado»[73].

Por último, me referiré a un supuesto que se repite con gran frecuencia, el de las cámaras simuladas que se instalan en propiedades particulares y parecen captar también zonas públicas o estar enfocadas directamente a la vía pública o propiedades de los vecinos. En los casos analizados que han sido objeto de denuncia ante la AEPD, la mayor parte de las instalaciones de este tipo responden a la intención de defensa frente al vandalismo en general o frente a las intrusiones de vecinos, atestiguados por lo general mediante denuncias presentadas por estos hechos. En ningún momento existe la pretensión de captar imágenes del exterior, pues los dispositivos suelen ser falsas cámaras o cámaras aptas para la grabación pero que están desconectadas e inactivas. La decisión de la AEPD ha sido siempre la misma, archivar las actuaciones por no existir realmente tratamiento de datos[74]. Lo que ha cambiado desde noviembre de 2015 en estos supuestos es que con anterioridad a esta fecha la AEPD instaba al particular a redirigir el dispositivo e, incluso, retirarlo porque «podía generar una situación de alarma entre las personas, que entendían que eran vigiladas a través de dichos dispositivos, al producirse una apariencia de tratamiento»[75]. Sin embargo, en los últimos años la AEPD no insta a su retirada, pues en realidad no hay riesgo de que se produzca tratamiento alguno de datos[76]. El cambio de criterio nos parece acertado, pues, aunque genere la

referencia pueda entenderse efectuada, con carácter general a la vía pública». Resolución de 11 de enero de 2018 (Expediente nº E/03264/2017), FD IV (p. 5).

73 Resolución de 14 de junio de 2017 (Expediente nº E/04934/2016), FD III (p. 8).

74 *Vid*., por ejemplo, Resolución de 6 de febrero de 2017 (Expediente nº E/03460/2016), Resolución de 17 de febrero de 2017 (Expediente nº E/03463/2016), Resolución de 22 de febrero de 2017 (Expediente nº E/03401/2016), Resolución de 28 de febrero de 2017 (Expediente nº E/05205/2016), Resolución de 3 de marzo de 2017 (Expediente nº E/05917/2016), Resolución de 31 de marzo de 2017 (Expediente nº E/04392/2016), etc.

75 Resolución de 26 de enero de 2018 (Expediente nº E/01925/2017), FD IV, p. 5.

76 «Esta Agencia consideró necesario revisar el mencionado criterio, en los términos que se plasman, entre otras, en la resolución del PS/00542/2015 de fecha 11 de noviembre de 2015. De este modo, la inexistencia de prueba alguna acerca de un posible de datos de carácter personal implica que la presente resolución de archivo no incorpore ningún tipo de requerimiento en el sentido que se ha mencionado, al prevalecer el principio de presunción de inocencia». *Ibid*.

sensación de vigilancia, reporta seguridad en zonas que suelen ser conflictivas socialmente sin que se produzca en realidad una intromisión en la privacidad de las personas.

3.3. *Cámaras instaladas en vehículos y drones*

Ya hemos afirmado que la captación de imágenes en un contexto personal o familiar en espacios públicos en las que aparecen terceros de forma accesoria no queda sometida a la aplicación de las normas de protección siempre que permanezcan en los ámbitos mencionados. De igual modo, tampoco quedaría sometida a la normativa la captación de imágenes en espacios públicos cuando las personas que aparezcan en ella de modo accesorio no sean identificables[77]. Sin embargo, pueden existir diferencias relevantes entre estos supuestos y la captación de imágenes en espacios públicos mediante cámaras *on board* o instaladas en drones, cuya finalidad no suele ser la de conservar un recuerdo de un momento familiar o de amistad, sino otra muy distinta que por lo general supone un uso posterior que supera tales ámbitos.

En el caso de las cámaras *on board* instaladas en vehículos, la finalidad suele ser de videovigilancia por motivos de seguridad durante su estacionamiento, o bien la de grabar las infracciones cometidas por otros vehículos con el fin de poderlas aportar posteriormente como prueba en posibles procedimientos sancionadores o judiciales. Esta suele ser también la finalidad de las grabaciones con cámaras instaladas por motoristas o ciclistas en sus cascos, que suelen activar la grabación en el momento en que se comete la infracción por parte de un tercero. Aunque esta sea la finalidad más probable, sin embargo, no podemos descartar que también pueda existir una finalidad doméstica en algunas ocasiones, por ejemplo, la grabación de una excursión familiar de la que se desea guardar un recuerdo. En estos supuestos, la consideración que merece es la misma que la grabación de una escena familiar con un móvil en una zona pública con captación accesoria e incidental de terceros, es decir, se trataría de una actividad doméstica excluida de la apli-

77 La AEPD, en su Informe 0153/2014 sobre la captación panorámica de espacios urbanos con cámaras sin utilización de zoom o herramientas que permitieran aproximación a los transeúntes, entendía que tales tratamientos no estarían sometidos a la normativa de protección por la imposibilidad de identificar a las personas que aparecían de modo accesorio.

cación de la normativa de protección de datos (siempre que no sean puestas a disposición de terceros).

En cuanto a las grabaciones con la finalidad de videovigilancia o aportación posterior de pruebas, a tenor de lo señalado por el TJUE en la ya citada sentencia de 11 de diciembre de 2014 (asunto C-212/13), nos encontraríamos ante una actividad incalificable como *exclusivamente* personal o doméstica, por lo que no encontraría amparo en la excepción recogida en el artículo 2.2.c) RGPD[78]. Este supuesto ni siquiera sería equiparable con la captación fortuita, en el curso de una grabación doméstica, de imágenes de la comisión de una infracción por un tercero, que podría acompañar a la denuncia formulada ante la autoridad competente o ser utilizada posteriormente como medio de prueba[79].

Con motivo de la entrada en vigor del RGPD, la AEPD ha publicado en 2018 un nuevo Informe de su Gabinete Jurídico[80] que coincide en gran medida con el contenido de su anterior Informe de 2015. El nuevo Informe analiza el desarrollo de esta actividad con la finalidad genérica de obtener pruebas que avalen posibles denuncias por supuestas infracciones de tráfico, llegando a la conclusión de que no estaría amparado por la excepción doméstica, pero podría estar amparado por el artículo 6.1.f) RGPD, es decir, la garantía de un interés legítimo (tutela judicial efectiva) siempre que no implique la vulneración de derechos fundamentales de los demás ciudadanos y cumpla los requisitos exigidos (información, etc.) para su legalidad[81].

---

78 En este sentido se pronunció de forma explícita la AEPD en su Informe 0456/2015 sobre cámaras *on board*. También la Agencia Vasca de Protección de Datos, en su Dictamen nº D16-040, de 29 de julio de 2016, Relativo a la adecuación a la normativa de protección de datos de las grabaciones de imágenes realizadas por particulares en vía pública sin consentimiento de los afectados, mediante la instalación de cámaras en vehículos o bicicletas, afirmaba que «la utilización de cámaras por particulares con fines de vigilancia en la vía pública, con independencia de que se realice desde un vehículo, una bicicleta, un dron, corriendo o caminando, no tiene encaje en la tan citada excepción; la vigilancia de la conducta ajena mediante cámaras no es algo subsumible en el ámbito particular, familiar o de amistad, tanto es así, que cuando se realiza afectando a la vía pública compete a las Fuerzas y Cuerpos de Seguridad» (pp. 9-10).

79 Cfr. Velasco Núñez, E., «Derecho a la imagen: tratamiento procesal penal», *Diario La Ley*, nº 8595 (2015), pp. 25-27.

80 *Vid*. Informe AEPD https://www.aepd.es/media/informes/informe-juridico-rgpd-camaras-on-board.pdf [consulta: 31-05-2018].

81 En el Informe se descarta que se puedan utilizar las cámaras *on board* con esta finalidad si no se incorporan ciertas garantías (p. 6), como, por ejemplo, que sólo se utilice en vehículos con licencias para el transporte de mercancías o personas, que se active únicamente cuando se produzca un evento concreto, que la grabación de imágenes se limite a los 20 segundos anteriores y posteriores al evento, etc. (pp. 6-7).

En cuanto al uso de drones, durante los últimos años se ha hecho cada vez más frecuente la dotación de estas aeronaves pilotadas a distancia con tecnología que puede implicar un alto riesgo para la privacidad, lo que llevó al GT29 a adoptar en el año 2015 un Dictamen sobre privacidad y protección de datos en relación al uso de drones[82]. También el Gabinete Jurídico de la AEPD ha publicado un Informe de 2018 que sigue en gran medida y completa el citado Dictamen[83].

Comienza poniendo de relieve el GT29 que los avances tecnológicos han facilitado dotar a los drones con equipos de grabación visual tan sofisticados que hacen posible el almacenamiento o transmisión de imágenes de gran calidad que permiten el reconocimiento facial, de las matrículas de los vehículos, la geolocalización de personas, sus movimientos, etc., sin que los afectados puedan sospechar siquiera que están siendo observados o grabados[84]. Incluso en el supuesto de que el ciudadano fuera consciente de la cercanía de un dron, le resultaría difícil advertir que está dotado de cámaras y, más aún, «saber qué datos serán tratados por los equipos de *a bordo*, con qué fines serán recogidos y por quién. Esto dará lugar a un aumento de la sensación de estar bajo vigilancia y una posterior disminución en el ejercicio legítimo de las libertades y los derechos civiles, más conocido como *efecto paralizante*»[85]. Resulta muy difícil, además, poder informar sobre estos extremos a quienes se puedan ver afectados[86].

---

82 Opinion (Dictamen) 1/2015, on Privacy and Data Protection Issues relating to the utilisation of Drones, WP 231, adoptado el 16 de junio de 2015 (hasta el momento sólo contamos con la versión inglesa).

83 *Vid*. Informe AEPD https://www.aepd.es/media/informes/informe-juridico-rgpd-drones.pdf (última consulta: 31.05.2018).

84 Cfr. Dictamen 1/2015, pp. 6-7.

85 «In any event, even if individuals are aware that a drone is in the area it is difficult to know which data processing equipment are on-board, for what purposes they are being collected and by whom. This will result in an increased feeling of being under surveillance and a subsequent possible decrease in the legitimate exercise of civil liberties and rights, best known as *chilling effect*». Dictamen 1/2015, p. 7.

86 En este sentido, la AEPD recoge en su informe de 2018 sobre drones que, dada esta dificultad, «En todo caso, esta valoración sobre el cumplimiento del derecho de información podría incluirse en una evaluación de impacto de protección de datos (EIPD). Dicho estudio de impacto deberá servir a los responsables y operadores para descubrir los riesgos a la privacidad asociados con el uso de la tecnología y procedimientos para el concreto tratamiento de datos que se pretende realizar. Dicho estudio de impacto deberá evaluar si el tratamiento de los datos personales por la vía solicitada es legítimo, necesario y proporcionado, así como deberá cubrir entre otros los aspectos de transparencia y seguridad y documentar los pasos que se han de tomar para minimizar los riesgos que aparezcan de dicho estudio de impacto». Informe AEPD citado, p. 6.

El GT29 admite que las captaciones de datos realizadas en espacios públicos mediante drones pueden tener en algunos supuestos carácter personal o doméstico, por ejemplo, cuando no haga posible la identificación de las personas o de las matrículas de los vehículos, o cuando, siendo esto posible, se trate de imágenes accesorias que no van a salir del ámbito doméstico, etc. Pensemos, por ejemplo, en el padre que, en lugar de grabar con una cámara manual (un teléfono móvil, por ejemplo) imágenes de un encuentro deportivo en el que participa su hijo, lo hiciera mediante un dron con la única finalidad de guardar un recuerdo del evento. No obstante, incluso en estos supuestos entiende el GT29 que deben ser tenidos en consideración los principios de proporcionalidad, calidad y minimización de datos (recogidos en el artículo 5.1 RGPD) para evitar una intromisión excesiva en la privacidad de otros participantes y de los espectadores. En este sentido recomienda, por ejemplo, que cuando se utilicen drones equipados con cámaras se incorporen las instrucciones necesarias para procesar automáticamente las imágenes con técnicas de visión borrosa u otros efectos gráficos que eviten la captación de imágenes de personas identificables[87]. Por su parte, la AEPD insiste, siguiendo al GT29, en que el primer requisito que debe cumplir quien desee llevar a cabo estos tratamientos es el de ajustarse al resto de la legislación que regula el uso de los drones[88], de ahí que, aunque se trate de un vídeo familiar, «cuando la operación de un dron viole la normativa nacional de aviación a la que está sujeta, o cualquier otra a la que deba atenerse, se considerará que la captación de datos y el tratamiento de los mismos realizados durante las operaciones aéreas no cumple con el principio de licitud recogido en el RGPD»[89].

---

87 «For example, when using drones equipped with video cameras, technical arrangements could be used by controllers to automatically process the images by using blurring or other graphical effects, in order to avoid the collection of images of identifiable persons whenever they are not necessary». Dictamen 1/2015, p. 14.

88 «En España la regulación actual en materia de drones está establecida en la ley 18/2014 de 15 de octubre, ya citada, proveniente del Real Decreto Ley 8/2014, de 4 de julio, que establece una normativa sustantiva al respecto y que a la vez modifica la Ley de Navegación Aérea, ley 48/1960, de 21 de julio, así como el Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea». Informe 2018 AEPD citado, p. 7.

89 Informe AEPD citado, p. 7.

Al margen de los supuestos citados, cualquier tratamiento efectuado mediante drones dotados con sistemas de captación o grabación de imágenes queda excluido de la excepción doméstica, debiendo cumplir todas las exigencias establecidas en la normativa de protección de datos de carácter personal[90].

4. Conclusiones

La protección de los datos de carácter personal continúa siendo una necesidad esencial para nuestra sociedad por la repercusión que puede tener sobre la intimidad y la vida privada de las personas el uso abusivo de los datos por parte de terceros, ya se trate de una administración pública, de empresas privadas o de personas particulares. Pudimos seguir en la prensa el escándalo derivado del uso indebido de los datos de los usuarios de Facebook por la empresa Cambridge Analitycs, pero esto es solamente un botón de muestra. Cada vez es más frecuente que las empresas que ofrecen servicios en red obtengan datos de los usuarios con fines comerciales fundamentalmente, en unas ocasiones con consentimiento y en otras sin él. También es frecuente el rastreo en redes sociales de los contenidos y perfiles abiertos de los usuarios con intereses comerciales, publicitarios, políticos, etc. En estos supuestos lo más grave no es el análisis de los datos del usuario que permite el acceso a ellos, sino los datos de personas cercanas a él por una relación familiar o de amistad que figuran en los contenidos subidos por ese usuario.

Por ello, es lógico que la UE haya querido acomodar la normativa de protección de datos a los nuevos riesgos introducidos por los avances tecnológicos, reforzando aquellos aspectos que la realidad misma mostraba como más débiles. El RGPD es una muestra de ello, aunque queda por ver todavía si la nueva regulación será realmente eficaz.

A pesar de la necesidad de reforzar la protección de los datos personales, sin embargo, no puede ser absoluta porque choca en ocasiones con otros derechos individuales de las esferas de la autonomía personal, de ahí que el legislador haya excluido del ámbito de aplicación de la normativa, entre otras materias, las actividades exclusivamente personales o domésticas. Sería ilógi-

---

90 *Vid*. más extensamente Pauner, C.; Viguri, J., «A Legal Approach to Civilian Use of Drones in Europe. Privacy and Personal Data Protection Concerns», *DS*, anno V, 5 (2015), pp. 85-121.

co, por ejemplo, exigir a un padre que graba con su móvil a su familia en una plaza pública que informe a todos los transeúntes sobre lo que está haciendo, o exigir el cumplimiento de determinados requisitos para elaborar una agenda o directorio personal de los amigos, o para elaborar el listado de los invitados a una boda, etc. Algo así ahogaría la libertad de las personas y supondría un control sobre las propias personas, no sobre los datos.

El carácter vago o un tanto indeterminado de la expresión «actividad personal o doméstica» ha motivado que los tribunales, los organismos especializados en la materia y la doctrina hayan debido concretar a lo largo de los últimos años los contornos de tales actividades. Es una lástima que el RGPD, que ha recogido la excepción doméstica tan escuetamente como lo hacía la Directiva derogada, no haya incorporado alguna de estas precisiones, en particular sobre las cuestiones más conflictivas. Esta omisión no constituye, sin embargo, un peligro para la seguridad jurídica, pues contamos con una experiencia suficiente para poder ofrecer a los aplicadores del Derecho y a los ciudadanos unos criterios sólidos sobre lo que deba entenderse como actividad personal o doméstica en las cuestiones más controvertidas, como, por ejemplo, el uso de las redes sociales, o de las cámaras en sus diversas posibilidades de utilización, o sobre los materiales que pueden ser colgados en webs, blogs, etc.

Bibliografía

Guasch Porta, V. y Soler Fuensanta, J.R., «El interés legítimo en la protección de datos», *Revista de Derecho UNED*, 16 (2015), pp. 417-438.

Leenes, R., «¿Quién controla la nube?», *IDP Revista de Internet, Derecho y Política* (UOC), 11 (2010), pp. 2-13.

Pauner, C. y Viguri, J., «A Legal Approach to Civilian Use of Drones in Europe. Privacy and Personal Data Protection Concerns», *DS*, anno V, 5 (2015), pp. 85-121.

Rallo Lombarte, A. y Martínez Martínez, R., «Protección de datos personales y redes sociales: obligaciones para los medios de comunicación», *Quaderns del CAC* 37, XIV (2) (2011), pp. 41-51.

Troncoso Reigada, A., «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales» (Parte una), *IDP Revista de Internet, Derecho y Política* (UOC), 15 (2012), pp. 61-75.

Velasco Núñez, E., «Derecho a la imagen: tratamiento procesal penal», *Diario La Ley*, nº 8595 (ref. D-311) (2015), pp. 1-37.

Dictámenes del Grupo de Trabajo del artículo 29 citados

Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, WP 89, adoptado el 11 de febrero de 2004.

Dictamen 4/2007 sobre el concepto de datos personales, WP 136, adoptado el 20 de junio de 2007.

Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas), WP 160, adoptado el 11 de febrero de 2009.

Dictamen 5/2009 sobre las redes sociales en línea, WP 163, adoptado el 12 de junio de 2009.

Opinion (Dictamen) 1/2015, on Privacy and Data Protection Issues relating to the utilisation of Drones, WP 231, adoptado el 16 de junio de 2015.