



Expediente Nº: E/01829/2012

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante las entidades GOOGLE, INC y GOOGLE SPAIN, S.L., de oficio y en virtud de denuncia presentada por la entidad PRIVACIDAD EN INTERNET S.L., y teniendo como base los siguientes,

HECHOS

PRIMERO: Entre los servicios ofrecidos por la entidad GOOGLE Inc., complementario del servicio "Google Maps", figura el denominado "Google Street View", que permite observar imágenes de las calles y carreteras de numerosos países del mundo, entre los que se encuentra España. Las imágenes que utiliza el servicio son captadas por una flota de vehículos que recorren las carreteras y calles dentro del denominado "Proyecto Google Street View", del que es responsable igualmente la entidad GOOGLE Inc., que ha dispuesto los equipos y diseñado el software empleado en la captación de información y creado los ficheros en los que se registra la misma para su posterior utilización a través de la red.

En relación con dicho servicio y, en concreto, con la recogida de datos personales que lleva a cabo en España, durante los meses de mayo a julio de 2010 se realizaron actuaciones de investigación dirigidas a sustanciar la eventual actividad infractora de Google que, mediante los coches habilitados para fotografiar las calles de distintas ciudades del mundo, para la aplicación Street View y al margen de esta función, recopiló datos de localización de las redes WI-FI, los datos SSID (identificador de la Red que, en ocasiones, coincide con el nombre real del abonado de la ed), las direcciones MAC, (los números que identifican la dirección fija de los dispositivos router) y datos de tráfico asociados a las redes WI-FI (datos transferidos mediante redes abiertas).

La captación de señales de redes inalámbricas, atendiendo a la naturaleza de la información registrada, se estimó como una recogida de datos de carácter personal, al tratarse de información concerniente a personas físicas identificadas o identificables. Ello determinó la apertura de un procedimiento sancionador a las entidades GOOGLE SPAIN, S.L. y GOOGLE Inc., señalado con el número PS/00541/2010.

Este procedimiento sancionador actualmente se encuentra suspendido por su vinculación con actuaciones que, por los mismos hechos, se están desarrollando en el orden jurisdiccional penal por parte del juzgado de Instrucción número 45 de Madrid.

SEGUNDO: Al margen del procedimiento expuesto, con fecha 09/03/2012, tuvo entrada en esta Agencia un correo electrónico remitido por GOOGLE Inc., en el que informó sobre el inicio en España de una nueva campaña de recogida de imágenes por parte de los vehículos del servicio "Street View", previsto para finales de ese mismo mes de marzo, que tenía el propósito de cubrir las zonas no cubiertas en las anteriores campañas realizadas entre los años 2008 y 2011.

Conocida la reanudación de dicho proyecto, con fecha 14/03/2012, se acordó el inicio de



las actuaciones previas de investigación de referencia, con objeto de analizar la adecuación a la normativa de protección de datos de carácter personal de los procedimientos de recogida y tratamiento de datos por parte del citado servicio.

TERCERO: Con fecha de 10/05/2012, tuvo entrada un escrito de la entidad Privacidad en Internet, S.L., en relación con una nota de prensa publicada por esta Agencia para informar sobre las actuaciones de investigación iniciadas. En dicho escrito, Privacidad en Internet, S.L. realiza las siguientes manifestaciones:

1. Entiende que esta Agencia está autorizando la captación, mediante la utilización de sistemas informáticos y ópticos, y medios para su tratamiento situados en territorio español, de imágenes de personas, matrículas de vehículos y cualesquiera otros datos personales que pudieran figurar en la vía pública, con destino a ser publicadas en Internet.
2. Dado que las imágenes captadas contienen datos de carácter personal y que la normativa española de protección de datos es aplicable a la GOOGLE Inc. en calidad de responsable del tratamiento, dicha entidad está infringiendo lo dispuesto en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), en tanto carece del consentimiento de las personas que aparecen en las imágenes captadas por sus vehículos.
3. El hecho de que las imágenes publicadas en Internet aparezcan con la información personal difuminada no exime a GOOGLE Inc. de la necesidad de recabar el consentimiento previo de quienes aparecen en ellas, ya que para poder realizar la tarea de difuminación previamente es necesario tener una imagen original.
4. Algunas de las imágenes han sido publicadas sin que el proceso de difuminado se haya aplicado y dicha publicación infringe lo dispuesto en el artículo 10 de la LOPD, al vulnerar el deber de secreto del responsable del tratamiento.
5. En la nota de prensa se indica que la Agencia ha solicitado a GOOGLE Inc. la inscripción de un fichero en el Registro General de Protección de Datos, por lo que entiende que ésta ha vulnerado lo previsto en el artículo 26.1 de la LOPD al no haberlo hecho con anterioridad al inicio del servicio en el año 2008.

El escrito adjunta 8 capturas de pantalla del servicio Street View en las que se muestran personas o matrículas de vehículos sin difuminar en distintas localizaciones de Madrid y Barcelona.

CUARTO: Por los Servicios de Inspección de la Agencia Española de Protección de Datos se realizaron diversos requerimientos de información a las entidades GOOGLE SPAIN y GOOGLE Inc., todos ellos respondidos por la última entidad citada, así como a la entidad Eurovendex, S.A., que presta el servicio de conducción de los vehículos "Street View" por virtud de un contrato suscrito con GOOGLE SPAIN.

Por otra parte, en visita de inspección, los servicios de la Agencia accedieron a uno de los vehículos utilizados en la recogida de datos para examinar los equipos físicos y lógicos utilizados. A esta inspección, según el detalle que consta en el acta de inspección elaborada, asistió la Directora de la Asesoría Jurídica de GOOGLE SPAIN, el Ingeniero de Operaciones Corporativas de Google Suiza, el Coordinador del Proyecto Street View en Europa, empleado en Google Suiza, un conductor contratado por Eurovendex, S.A. y un asesor jurídico externo de Google Inc.

Finalmente, los Servicios de Inspección accedieron al servicio "Google Street View" prestado a través de Internet para obtener, mediante una búsqueda manual, una muestra de imágenes publicadas y verificar su estado.



QUINTO: Como resultado de la fase previa de investigación desarrollada para el esclarecimiento de los hechos, los servicios de inspección de la Agencia Española de Protección de Datos informaron lo siguiente:

1. "Google Street View" es un servicio ofrecido por GOOGLE Inc., complementario del servicio "Google Maps", que permite observar imágenes de las calles y carreteras de numerosos países del mundo entre los que se encuentra España.
2. Dentro de la actual campaña, la recogida de datos que permiten ofrecer y mejorar este servicio se realiza mediante un conjunto de aproximadamente 20 vehículos, equipados cada uno de ellos con 15 cámaras fotográficas digitales y un grupo de sensores laser y de posicionamiento.
3. Consultados los representantes de la entidad GOOGLE Inc. sobre la frecuencia de captación de imágenes, éstos manifestaron que no existe una frecuencia fija sino que varía en función de la velocidad del vehículo, siendo el mínimo un conjunto de imágenes (una por cámara) cada 8 segundos y el máximo de 4 conjuntos por segundo en el caso de que el coche circule a más de 40 m/s.
4. Con fecha 17/05/2012, la inspección actuante realizó una búsqueda manual de imágenes en las que se mostrasen matrículas de vehículos y rostros de personas no difuminados, principalmente en áreas con alta probabilidad de aparición de transeúntes, como plazas y calles peatonales. La búsqueda dio como resultado dos matrículas y una decena de rostros no difuminados.
5. Las imágenes mostradas por el servicio Street View disponen de un enlace que permite informar al responsable del servicio de diferentes tipos de error en la imagen que se está mostrando en ese momento. El enlace conduce a una página que nos permite resaltar el área en la que se encuentra el error y aportar información sobre el tipo de error a notificar. Entre los tipos de errores sobre los que se puede informar están los relacionados con la privacidad, los de contenido inapropiado y un tercer apartado de "otros".
Dentro del primer grupo, el sistema ofrece la posibilidad de indicar si el problema radica en que la imagen muestra una cara, un edificio, un coche o una matrícula sin difuminar. Una vez realizada la solicitud de corrección, se remite de manera automática un correo electrónico a la dirección de correo facilitada, en el que se informa que las imágenes están en proceso de revisión.
Los servicios de inspección solicitaron la revisión de una imagen que mostraba una cara sin difuminar el viernes 2 de noviembre de 2012. La solicitud fue resuelta el sábado 3 de noviembre, indicando que los cambios podrían tardar 24 horas en ser visibles. El lunes 5 de noviembre de verificó que efectivamente la cara estaba difuminada.

Respecto a la inscripción de ficheros en el Registro General de Protección de Datos

6. El 11/05/2012, GOOGLE Inc. solicitó la inscripción de un fichero denominado "GOOGLE STREET VIEW" en el Registro General de Protección de Datos, que finalmente fue inscrito el 15 de mayo.
La finalidad del citado fichero es *"Fotografiar calles con fines de cartografía, pudiendo incidentalmente captarse la imagen de personas o vehículos, con sujeción a un sistema de difuminado y fotografiar calles con la finalidad de publicarlas en el servicio de "Street View", pudiendo captarse incidentalmente la imagen de personas o vehículos, con sujeción a un sistema de difuminado"*, figurando GOOGLE Inc. como responsable del fichero y GOOGLE SPAIN, S.L. como entidad a la que dirigirse a la hora de ejercer los derechos ARCO.

Respecto de los tipos de datos recabados

7. Los vehículos recaban únicamente imágenes fotográficas, datos telemétricos y escaneados



laser tridimensionales.

A diferencia del precedente reseñado en el Antecedente Primero, no se recogen datos transmitidos a través de redes inalámbricas. Durante la inspección realizada el 05/09/2012 a uno de los vehículos utilizados durante la campaña de recogida de datos no se han hallado elementos hardware o software que pudiesen ser utilizados para la recolección de datos transmitidos a través de redes inalámbricas. Tampoco se localizó ningún fichero que almacenase datos de redes inalámbricas.

En la copia de la documentación proporcionada a los conductores de los vehículos tampoco se incluye ninguna referencia a hardware o software alguno cuya función sea la recogida de datos transmitidos a través de redes inalámbricas.

Además, GOOGLE Inc. ha aportado copia de un memorando elaborado el 25/03/2011 por la empresa auditora Stroz Friedberg LLC, que fue la que realizó en el año 2010 el informe sobre el software utilizado en la recogida de datos transmitidos a través de redes inalámbricas. En dicho memorando, la entidad informa sobre el resultado de la inspección a un vehículo del servicio Google Street View que confirma que el equipamiento instalado en dicho vehículo no permite la recogida de datos de redes inalámbricas basadas en el protocolo 802.11 (también conocido como WiFi).

Respecto de las entidades intervinientes

8. Los representantes de GOOGLE Inc. manifiestan que es dicha entidad la *“...responsable de toda la recogida y tratamiento de los datos que pudieran ser recogidos como parte del servicio Street View en España”* pero durante la citada inspección pudo verificarse que, al igual que en el caso del coche inspeccionado en relación con el expediente E/01482/2010, el permiso de circulación del vehículo está a nombre de GOOGLE SPAIN, S.L.

Al respecto, los representantes de GOOGLE Inc. manifiestan que *“Los coches Street View y sus equipos están bajo control operacional de Google Inc. Tanto los coches como los equipos instalados en ellos fueron proporcionados y pertenecen a Google Spain, que actúa en nombre de Google Inc. que es “la entidad responsable del desarrollo e implementación del proyecto [Street View]”*.

9. La operación de los vehículos del servicio corre a cargo de conductores que son empleados de la empresa EUROVENDEX, S.A.

Los contratos de los servicios de conducción de los vehículos son, según manifiesta GOOGLE Inc., los analizados en el expediente E/01482/2010 y se estructuran en base a:

Un contrato marco firmado el 3 de abril de 2008 entre GOOGLE Inc. y ADDECO USA, Inc. con el fin de que esta última, o alguna de sus filiales, proporcione trabajadores temporales a GOOGLE Inc., o a alguna de sus filiales.

Un contrato firmado el 13/05/2008 entre GOOGLE SPAIN, S.L. y EUROVENDEX, S.A. que concreta el contrato marco anterior para el caso de España.

10. El director del proyecto Street View en España es un empleado de Google Suiza, filial de la compañía con sede en Zurich y, según manifiesta Google Inc., actúa bajo su dirección y control último.

Respecto de los tratamientos de datos realizados

Los representantes de GOOGLE Inc. manifestaron lo siguiente:

11. Los datos recabados mediante los sensores de los vehículos son almacenados en discos duros que los conductores de éstos remiten a la sede de la filial de Google en Bélgica para que sean cargados en los servidores seguros que allí se encuentran.

12. *“Las imágenes de Street View sin difuminar recogidas en España podrán ser transferidas desde su lugar de almacenamiento en los servidores de Google Inc. en Bélgica, a un lugar de almacenamiento en los servidores de Google Inc. ubicados en Estados Unidos, donde la información se almacena y procesa conforme a los principios de Puerto Seguro.”*



13. El procesamiento de los datos incluye:
- La decodificación y conversión de las imágenes, que originalmente se obtiene en un formato RAW (formato de archivo digital de imágenes que contiene la totalidad de los datos de la imagen tal y como ha sido captada por el sensor digital de la cámara fotográfica. No existe un formato estándar sino que cada fabricante de cámaras usa su propia versión del formato), a formato JPEG.
 - Selección inicial de imágenes para descartar las que se consideren no adecuadas para su publicación.
 - El almacenamiento de las imágenes sin difuminar
 - La aplicación de tecnología de difuminado a los rostros de las personas que sean identificables y a las matrículas de vehículos que sean legibles.
 - El juntado (“stitching”) y mezcla (“blending”) de imágenes para crear imágenes panorámicas.
 - La aplicación de correcciones de color.
 - La extracción de información geográfica de las imágenes con el fin de mejorar Google Maps.
14. El Coordinador del Proyecto Street View en Europa manifestó durante la inspección realizada que el procesamiento completo de los datos recogidos en España, incluyendo la difuminación de las caras y matrículas, puede realizarse y se realiza habitualmente en el centro de proceso de datos de Google en Bélgica aunque, en función de las circunstancias, ese mismo procesamiento podría ser realizado en los centros de proceso de datos de Google en los Estados Unidos.
15. GOOGLE Inc. mantiene una copia sin difuminar de las imágenes publicadas durante un periodo máximo de un año, a contar desde la publicación de las mismas.
GOOGLE Inc. justifica la conservación de las imágenes originales aduciendo que la tecnología de difuminado automático afecta de manera frecuente a nombres de calles y otras señalizaciones que se utilizan para realizar los mapas de forma precisa al confundirlas con matrículas de coches.

Respecto del acceso a los datos recabados

16. Los conductores de los vehículos no tienen acceso a las imágenes recogidas y a los datos asociados a éstas, aparte de la posibilidad de ver, de forma temporal imágenes de baja resolución de control de calidad, que se muestran en el sistema de recogida del propio vehículo.
El “Manual del conductor” indica en su punto 4.9 “Control de calidad” que *“Una imagen de control [...] es una instantánea de lo que ven todas las cámaras en ese momento, que se muestra de forma automática en la pantalla cuando se empieza a conducir y cada cinco o diez minutos. Para activar la visualización de las imágenes de QC también se puede pulsar”*.
17. El resto de empleados de EUROVENDEX, S.A. no tiene acceso a los datos recogidos.
18. Durante la inspección realizada el 05/09/2012 se pudo comprobar que el disco en el que se almacenan los datos recogidos por el vehículo está bloqueado de forma que requiere de una clave de acceso y de un software adecuado (que no puede obtenerse fuera de las empresas del grupo Google) para poder acceder a su contenido.
19. El Director del proyecto Street View en España puede, bajo la dirección y control último de GOOGLE Inc. y de conformidad con el código de conducta de Google y sus directrices internas, tener acceso limitado a las imágenes y datos asociados una vez estas han sido descargadas en los servidores de Google en Bélgica.
El Director del proyecto Street View en España no puede eliminar ni modificar ninguna de las imágenes recogidas ni la información asociada.
20. Los empleados de Google Bélgica y GOOGLE Inc. que necesiten acceder a las imágenes para procesarlas lo hacen de conformidad con el código de conducta de Google y las



directrices internas descritas en el documento “Política de Acceso por Empleados” que establecen, entre otras cosas que:

- a. El acceso está restringido por un nombre de usuario y contraseña seguros y otras medidas de seguridad de redes.
- b. Google requiere el uso de una identificación de usuario única para cada empleado.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la LOPD.

II

Las presentes actuaciones tienen por objeto el análisis de las conductas realizadas por las entidades GOOGLE Inc. y GOOGLE SPAIN desde el punto de vista de la normativa de protección de datos de carácter personal, por la recogida de datos en el marco del proyecto “Google Street View”.

Procede analizar, en primer término, si la información captada incluye datos de carácter personal, considerando que el objeto de la LOPD señalado en su artículo 1 tiene que ver con la garantía y protección, en lo que concierne al tratamiento de datos personales, de las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La LOPD viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.

En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala que *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*. Por ello resulta preciso determinar que ha de entenderse por dato de carácter personal y tratamiento de datos.

El artículo 3.a) de la LOPD define el concepto de dato de carácter personal como *“cualquier información concerniente a personas físicas identificadas o identificables”*.

Y el apartado 1.f) del artículo 5 del Real Decreto 1720/2007, de 21 de diciembre (RLOPD), por el que se aprueba el Reglamento de desarrollo de la LOPD, define dato de carácter personal como *“cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables”*.

De ello se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable.

La definición de persona identificable aparece en la letra o) del citado artículo 5.1 del



RLOPD, que considera como tal *“toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados”*.

En relación con lo anterior, el artículo 2.a) de 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 datos personales y a la libre circulación de estos datos, considera identificable *“toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de la Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

Sobre este concepto, la Audiencia Nacional en su sentencia de 08/03/2002, ha señalado que *para que exista dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados, tal y como se desprende del mencionado artículo 3 de la Ley, en sus apartados a) y f) y también del Considerando 26 de la invocada Directiva 95/46/CE que expresamente señala que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado”*.

Atendiendo a la definición contenida en las normas citadas, que consideran dato de carácter personal *“cualquier información concerniente a personas físicas identificadas o identificables”*, la imagen fotográfica de una persona y el número de matrícula de un vehículo se ajustan a este concepto por cuanto permite la identificación de la persona afectada.

En relación con la imagen, la Directiva 95/46/CE en su Considerando 14 lo afirma expresamente al señalar lo siguiente:

“Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos”.

Es claro, pues, que para el legislador comunitario la imagen personal es un dato de carácter personal sujeto al régimen de protección establecido en la Directiva cuando se efectúe tratamiento sobre ella.

Y el artículo 5.1.f) del Real Decreto 1720/2007, antes citado, se refiere a *“cualquier información... fotográfica... concerniente a personas físicas identificadas o identificables”*.

La misma conclusión puede obtenerse respecto de los datos contenidos en la placa de matrícula de un vehículo, cuyo tratamiento se encontrará sometido a la LOPD por cuanto permiten la identificación de un individuo sin que ello exija plazos o esfuerzos desproporcionados.



El artículo 5 h) del Texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto Legislativo 339/1990, de 2 de marzo, establece que *“se atribuyen al Ministerio del Interior las siguientes competencias en el ámbito de esta Ley, sin perjuicio de las que tengan asumidas las Comunidades Autónomas en sus propios Estatutos (...) los registros de vehículos, de conductores e infractores, de profesionales de la enseñanza de la conducción, de centros de formación de conductores, de los centros de reconocimiento para conductores de vehículos a motor y de manipulación de placas de matrícula, en la forma que reglamentariamente se determine”*.

En consecuencia, el citado precepto reconoce la subsistencia del Registro de Vehículos, creado por el artículo 244 del Código de la Circulación, aprobado por Decreto de 25 de septiembre de 1934, habilitando expresamente al desarrollo reglamentario del Texto Refundido para establecer el régimen del citado Registro.

Dicho desarrollo se produjo a través de la aprobación del Reglamento General de Vehículos, en virtud de Real Decreto 2822/1998, de 23 de diciembre, cuyo artículo segundo establece en su párrafo primero que *“la Jefatura Central de Tráfico llevará un Registro de todos los vehículos matriculados, que adoptará para su funcionamiento medios informáticos y en el que figurarán, al menos, los datos que deben ser consignados obligatoriamente en el permiso o licencia de circulación, así como cuantas vicisitudes sufran posteriormente aquéllos o su titularidad”*.

En cuanto a su finalidad, el párrafo segundo del precepto previene que *“estará encaminado preferentemente a la identificación del titular del vehículo, al conocimiento de las características técnicas del mismo y de su aptitud para circular, a la comprobación de las inspecciones realizadas, de tener concertado el seguro obligatorio de automóviles y del cumplimiento de otras obligaciones legales, a la constatación del Parque de Vehículos y su distribución, y a otros fines estadísticos”*.

Por último, y en lo atinente a la publicidad de sus datos, el párrafo tercero del citado artículo 2 añade que *“el Registro de Vehículos... será público para los interesados y terceros que tengan interés legítimo y directo, mediante simples notas informativas o certificaciones”*. En consecuencia, se establece el carácter público del Registro, bastando para la consulta de sus datos la alegación de la existencia de un interés legítimo y directo en la consulta.

En consecuencia, cabe considerar que la identificación del titular del vehículo no exige esfuerzos o plazos desproporcionados, por lo que el tratamiento del dato de la matrícula habrá de ser considerado como tratamiento de un dato de carácter personal.

En definitiva, aplicando las normas expuestas, la información captada para el proyecto *“Google Street View”* se ajusta al concepto de dato de carácter personal, al tratarse de información concerniente a personas físicas identificables o identificables, ya que con los datos almacenados es posible la identificación de los titulares de los mismos sin un esfuerzo exagerado o desproporcionado.

Por otra parte, la aplicabilidad de la normativa de protección de datos de carácter personal, de acuerdo con lo indicado en el citado artículo 2.1 de la LOPD, requiere que dichos datos aparezcan registrados en un soporte físico que los haga susceptibles de tratamiento.

La interpretación de este precepto puede igualmente efectuarse a partir del ámbito de aplicación de la Directiva 95/46/CE, que dispone en su artículo 3.1 que *“Las disposiciones de la*



presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero”.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.*

Por tanto, la garantía del derecho a la protección de datos, conferida por la normativa de referencia requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

En el presente caso, se recogen datos personales mediante la utilización de los medios expresados y son registrados en ficheros automatizados que permiten su utilización posterior.

Por tanto, de conformidad con la normativa expuesta, la captación, grabación, transmisión, conservación, y almacenamiento de imágenes de personas de forma que permitan su identificación y de vehículos con el detalle de sus matrículas, con la finalidad expresada, constituye un tratamiento de datos personales que cae bajo la órbita de la normativa de protección de datos de carácter personal, toda vez que la información recogida contiene datos concernientes a personas identificadas o identificables situadas en el entorno fotografiado y sobre las que se aportan detalles relativos a la imagen personal de éstas, el lugar de su captación y la actividad o conducta desarrollada por los individuos a las que las imágenes se refieren.

De acuerdo con aquella definición de tratamiento de datos personales, la mera captación de imágenes de las personas y matrículas de vehículos puede considerarse un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada, en la medida en que dicho tratamiento se efectúa sobre información concerniente a personas físicas identificadas o identificables.

Así, en el presente supuesto, considerando que la información recogida permite la identificación de los afectados, debe concluirse la existencia de datos de carácter personal que son sometidos a tratamiento y la plena aplicabilidad de los principios y garantías expuestas en la normativa de protección de datos de carácter personal.

III

Atendiendo a las entidades implicadas, procede analizar el ámbito de aplicación de la LOPD respecto de los hechos imputados; cuestión de la que se derivan dos aspectos básicos como son la posible existencia o no de infracciones y la propia competencia de la Agencia Española de Protección de Datos para, en su caso, declararlas e imponer las sanciones legalmente previstas.

El examen de esta cuestión exige considerar si las conductas analizadas han sido llevadas a cabo en el marco de las actividades de un responsable del tratamiento en territorio español o se han empleado medios situados en España por parte de un responsable del tratamiento no establecido en la Unión Europea. Si nos encontrásemos en uno de estos casos serían aplicables los principios, derechos y garantías previstos en la legislación española de

protección de datos.

La LOPD, en el párrafo segundo de su artículo 2.1, al referirse al “Ámbito de aplicación” de la norma, establece lo siguiente:

“Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito”.

Y el último párrafo del artículo 5.1 de la misma norma establece lo siguiente:

“Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento”.

Por otra parte, el artículo 3 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2008, señala su ámbito territorial de aplicación en los siguientes términos:

“1.- Se regirá por el presente Reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente Reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2.- A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad”



En este mismo sentido se pronuncia el artículo 4 “Derecho nacional aplicable” de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que establece lo siguiente:

“Derecho nacional aplicable

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento”.

Este artículo responde a las consideraciones que se plasman en la exposición de motivos de la misma Directiva; en concreto los considerandos 18 y siguientes presentan la siguiente justificación del artículo 4 en cuestión:

“(18) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado;

(19) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;

(20) Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del

Estado miembro en el que se ubiquen los medios utilizados y deben adaptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;”

Conforme a lo dispuesto en el artículo 4.1.a) de la directiva, la aplicación de las disposiciones nacionales de un Estado miembro viene determinada por la existencia de un establecimiento del responsable del tratamiento en el territorio del Estado miembro de que se trate. Aunque esta Directiva no define el concepto de “establecimiento”, en su preámbulo (Considerando 19) señala como elemento determinante el ejercicio efectivo y real de actividades a través de una instalación estable, no siendo preciso que dicho establecimiento tenga personalidad jurídica. Además, el tratamiento de datos personales deberá llevarse a cabo en el marco de tales actividades.

En relación con esta cuestión, el Grupo de Trabajo del artículo 29, en su Dictamen 8/2010, sobre Derecho aplicable, emitido el 16/12/2010, señala que *“la referencia a «un» establecimiento significa que la aplicabilidad del Derecho de un Estado miembro se desencadenará por la ubicación de un establecimiento del responsable del tratamiento en ese Estado miembro y los Derechos de otros Estados miembros podrían desencadenarse por la ubicación de otros establecimientos de ese responsable del tratamiento en esos Estados miembros”*. Y añade que *“Aun cuando el responsable del tratamiento tenga su establecimiento principal en un tercer país, el mero hecho de tener uno de sus establecimientos en un Estado miembro podría desencadenar la aplicabilidad del Derecho de dicho país, siempre que se reúnan las otras condiciones del artículo 4, apartado 1, letra a)...”*.

El mismo Dictamen citado señala que *“la noción de “marco de actividades” no implica que el Derecho aplicable sea el del Estado miembro donde esté establecido el responsable del tratamiento, sino donde un establecimiento del responsable del tratamiento esté implicado en actividades relativas al tratamiento de datos”*, y que deberá tenerse en cuenta al respecto el grado de implicación del establecimiento en las actividades de tratamiento de datos personales.

En este caso, al margen de la forma jurídica de la entidad GOOGLE SPAIN, existe un establecimiento implicado en actividades que entrañan el tratamiento de datos personales relativos a personas identificadas o identificables, que se tratan y divulgan en territorio español.

El los Antecedentes de esta Resolución se describe detalladamente la participación de GOOGLE SPAIN en los hechos, que tiene relación directa con la recogida de datos personales en todo el territorio español, realizada en el ámbito de responsabilidad de dicha entidad. Para que dicha recogida de datos se pudiera llevar a efecto, GOOGLE SPAIN suscribió en su propio nombre un contrato de encargo del tratamiento con EUROVENDEX, en virtud del cual dispuso los vehículos equipados con la tecnología necesaria, indicó las áreas a cubrir, facilitó la formación inicial del personal de EUROVENDEX, designó las personas de contacto, realizó el pago de las facturas generadas por el servicio y asumió la responsabilidad de cumplir en todo el proceso con las obligaciones legales establecidas en la LOPD, exigiendo la implantación de las medidas de seguridad de nivel medio establecidas en la normativa de protección de datos.

Por lo tanto, dado que las investigaciones realizadas por la Inspección de Datos de la Agencia Española de Protección de Datos acreditan suficientemente que el tratamiento de datos consistente en la recogida de datos personales llevada a cabo por los vehículos empleados en el proyecto “Google Street View” ha sido realizado en el marco de las actividades de un establecimiento del responsable del tratamiento ubicado en territorio español, cabe concluir que la protección conferida por la LOPD es aplicable al presente supuesto y, por ende, la Agencia



Española de Protección de Datos es competente para la tramitación del presente procedimiento, de conformidad con lo establecido en el artículo 2.1.a) de la citada Ley Orgánica.

Aún cuando no resultara procedente la aplicación de lo dispuesto en el artículo 2.1.a) de la LOPD, también es competente la Agencia Española de Protección de Datos para decidir sobre el tratamiento llevado a cabo por un responsable no establecido en territorio del Espacio Económico Europeo que ha utilizado en el tratamiento de datos medios situados en territorio español y actuado por medio de representante, por lo que debe concluirse, igualmente, que la LOPD es aplicable al presente supuesto y procedente la intervención de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 2.1.c) de la LOPD, ya citado. De este modo, GOOGLE Inc. ha recurrido a medios situados en el territorio español, como son los equipos instalados en los vehículos empleados en el proyecto "Google Street View", con el fin de captar información en nuestro territorio. En este caso, la utilización de tales equipos para la recogida de datos no se realiza exclusivamente con fines de tránsito por el territorio de la Unión Europea, es decir, no se trata de equipos de transmisión, sino que dichos equipos se emplean para la recogida y tratamiento de los datos.

IV

En el supuesto examinado, se constata que los datos personales recogidos por los vehículos asignados al proyecto "Google Street View" son registrados en un fichero automatizado.

De acuerdo con el artículo 26.1 de la LOPD, según el cual *"Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos"*, deben notificarse a esta Agencia, para su inscripción en el Registro General de Protección de Datos, los ficheros que contengan datos de carácter personal.

A este respecto, el artículo 55.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD, dispone lo siguiente:

"2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos".

Y en el apartado del citado artículo 55 se añade lo siguiente:

"4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento".

Con fecha 11/05/2012, GOOGLE Inc. solicitó la inscripción de un fichero denominado "GOOGLE STREET VIEW" en el Registro General de Protección de Datos, que finalmente fue inscrito el 15 de mayo. La finalidad del citado fichero es *"Fotografiar calles con fines de cartografía, pudiendo incidentalmente captarse la imagen de personas o vehículos, con sujeción"*



a un sistema de difuminado y fotografiar calles con la finalidad de publicarlas en el servicio de "Street View", pudiendo captarse incidentalmente la imagen de personas o vehículos, con sujeción a un sistema de difuminado", figurando GOOGLE Inc. como responsable del fichero y GOOGLE SPAIN, S.L. como entidad a la que dirigirse a la hora de ejercer los derechos ARCO.

V

El artículo 6.1 de la LOPD dispone lo siguiente: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*.

Por su parte, el apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en aquel apartado 1, estableciendo que: *"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"*.

Estos preceptos, a su vez, se encuentran desarrollados por el artículo 10 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD, en el que se establece lo siguiente:

"Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de



derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concorra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud”.

A su vez, las disposiciones citadas deben ser interpretadas a la luz de las previsiones del artículo 7 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual:

“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva”.

Debe, en particular, tenerse en cuenta que la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 establece en su fallo que *“El artículo 7, letra f, de la Directiva tiene efecto directo”*. Por ello, dicho precepto deberá ser tomado directamente en cuenta en la aplicación de la normativa de protección de datos de carácter personal por los Estados Miembros, y en consecuencia por esta Agencia Española de Protección de Datos, dado que como señala el Tribunal Supremo en su sentencia de 8 de febrero de 2012 *“produce efectos jurídicos inmediatos sin necesidad de normas nacionales para su aplicación, y que por ello puede hacerse valer ante las autoridades administrativas y judiciales cuando se observe su trasgresión”*.

Indica la Sentencia Del TJUE, en su apartado 38, que el artículo 7.f) de la Directiva *“establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado”* y, en relación con la citada ponderación, el apartado 40 recuerda que la misma *“dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado”*.

Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión, por lo que, conforme a su apartado 47, *“nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación”*.

Estas previsiones exigen que, en aquellos supuestos en los que la legislación española haya establecido causas legitimadoras del tratamiento que no resulten plenamente coincidentes con las previstas en los apartados a) a e) del citado artículo 7 de la Directiva, será preciso valorar si procede aplicar la causa legitimadora establecida en dicho precepto, para lo cual habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 de la LOPD, según el cual *“la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”* o si, por el contrario, dichos derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar el tratamiento de los datos de carácter personal.

El artículo 7.f) de la Directiva 95/46/CE no puede ser interpretado en el sentido de que la mera invocación del interés legítimo del responsable pueda justificar por sí solo el tratamiento de los datos, sino que es necesario que el mencionado interés legítimo sea preponderante sobre los derechos e intereses de los afectados. Así lo ha puesto de manifiesto el Tribunal de Justicia de la Unión Europea en la tan repetida Sentencia de 24 de noviembre de 2011, tal y como se ha indicado en un lugar anterior de la presente resolución.

De este modo, el mero interés legítimo derivado de la simple voluntad de ejercer una



actividad empresarial no es suficiente para legitimar un tratamiento si una vez efectuado el juicio de ponderación impuesto por el artículo 7.f) de la Directiva han de prevalecer otros derechos fundamentales e intereses dignos de protección y, en particular, los derechos a la intimidad y a la protección de datos de carácter personal, consagrado por los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea y 18 de la Constitución. Ello impone que el interés legítimo invocado deba ostentar la relevancia necesaria para que quepa apreciar su prevalencia una vez llevada a cabo la mencionada ponderación.

VI

Procede analizar, por consiguiente, si existe un interés legítimo del responsable que ostente la relevancia necesaria en el sentido dispuesto en el artículo 7.f) de la Directiva 95/46/CE.

En este sentido, cabe apreciar que las actividades descritas en el presente procedimiento se enmarcan entre las contempladas en la Directiva 2000/31/CE que tiene por objeto impulsar el desarrollo de los servicios de la sociedad de la información como “medio esencial para eliminar las barreras que dividen a los europeos”; ofrecer nuevas oportunidades para el empleo y para el crecimiento de las empresas europeas, así como las inversiones en innovación (Considerandos 1 y 2). Para ello la Directiva establece un marco claro y de carácter general, “fundamental para garantizar la seguridad jurídica y la confianza de los consumidores” que “garantice la libre circulación de los servicios de la sociedad de la información” entre los Estados miembros (Considerandos 7 y 8).

Del interés de los servicios de la sociedad de la información cabe deducir, que existe un valor querido por el legislador, como es el desarrollo de la sociedad de la información, que deberá tenerse en cuenta en el análisis que se realice sobre la existencia de un interés legítimo prevalente así como las consecuencias que puedan derivarse para el derecho a la protección de datos de carácter personal, enteramente aplicable a dichos servicios.

Sin embargo, esta norma no contiene ninguna previsión que directamente legitime el tratamiento de datos llevado a cabo por las entidades GOOGLE SPAIN y GOOGLE Inc. para la prestación del servicio “Google Street View”. Tampoco el interés comercial vinculado al desarrollo de la actividad por sí mismo puede considerarse como un interés prevalente en el sentido exigido en el artículo 7.f) de la Directiva 95/46/CE.

No obstante, en el presente caso concurren otros elementos que deben ser tomados en consideración al ponderar el interés legítimo y los derechos e intereses de los afectados.

Así, debe tenerse en cuenta la finalidad del servicio. “Google Street View” es un servicio ofrecido como complemento del de “Google Maps”, que permite a los usuarios observar imágenes de las calles y carreteras de numerosos países del mundo, proporcionando panorámicas fotográficas de las mismas en el territorio de que se trate y procesadas para su publicación y para la creación de mapas.

De este modo, resulta evidente que la finalidad del proyecto “Google Street View” no es obtener información relativa a las personas, cuya recogida es incidental. Tampoco lo es la identificación de los afectados, ni el tratamiento posterior de dicha información para su divulgación. La finalidad última de la recogida de información llevada a cabo es la prestación de un servicio de cartografía.



Así mismo debe tomarse en cuenta para realizar esta ponderación otros elementos verificados en las actuaciones por los Servicios de Inspección de la Agencia, que se establecen para minimizar o evitar el riesgo para la intimidad de las personas. Entre ellos, cabe destacar los siguientes:

- En primer lugar, los programas diseñados para la recogida y proceso de los datos no disponen de instrumentos de reconocimiento facial ni permiten la búsqueda por personas.
- En segundo lugar, las imágenes que se ofrecen son estáticas y no identifican la fecha concreta de su captación.
- En tercer lugar, las imágenes de personas y vehículos se someten a un proceso de anonimización, previo a su publicación, consistente en difuminar los rostros y matrículas para evitar que puedan ser reconocidos.
- En cuarto lugar, únicamente se contempla la conservación o retención de los originales de las fotografías tomadas, en los que constan los datos personales, por el período necesario para la mejora del servicio o cumplimiento de los fines para los que fueron recabados, y previo a la destrucción de la información personal registrada, momento a partir del cual únicamente se conservan las imágenes anonimizadas.

Finalmente es necesario tomar en consideración el mecanismo habilitado a través de dirección de Internet <http://maps.google.es>....., que permite a cualquier afectado solicitar la corrección de cualquier error en el difuminado de rostros y matrículas de vehículos, cuya eficacia ha sido contrastada por los Servicios de Inspección.

En dicha URL se indica lo siguiente:

“Las personas y las matrículas de los coches se muestran difuminadas. Hemos desarrollado una tecnología vanguardista para difuminar las caras y las matrículas de los coches que se aplica a todas las imágenes de Street View. Esto significa que si una de nuestras imágenes contiene una cara (por ejemplo, de un transeúnte en la acera) o una matrícula identificable, nuestra tecnología difumina la imagen de forma automática, con el fin de que no se pueda identificar a la persona o al vehículo en particular. Si a nuestros detectores se les escapa algo, puedes informarnos fácilmente.”

Se establece de esta forma un cauce para posibilitar la supresión o corrección, con celeridad, del dato tratado. El afectado puede ejercitarlo ante el responsable del servicio, pudiendo para ello hacer uso de la funcionalidad “Reportar un problema” que GOOGLE ofrece en la parte inferior izquierda de la ventana de la imagen en cuestión, desde donde puede cumplimentarse un formulario para informar sobre una “imagen inadecuada”, Adicionalmente puede ejercer su derecho de cancelación ante Google Spain.

En el caso de que la solicitud no fuera convenientemente atendida, el afectado puede dirigirse a esta Agencia, acompañando copia de la solicitud cursada, de la documentación que acredite su recepción por el destinatario y, en el caso de que hubiese recaído, de la contestación recibida, para que, de conformidad con lo previsto en el artículo 18 de la Ley Orgánica, pueda analizarse la procedencia de tutelar su derecho, sin descartarse tampoco el recurso a la vía punitiva consistente en la incoación de un procedimiento sancionador en el supuesto de que, a pesar de haberse dictado una resolución de tutela estimando su reclamación, permanezcan los



datos y resulte procedente.

De conformidad con lo expresado, teniendo en cuenta todos los elementos de ponderación relacionados en el presente fundamento, no se aprecia que, con carácter general, la recogida de imágenes de personas y de matrículas de vehículos y su posterior tratamiento en el marco de las actividades de prestación del servicio "Google Street View", analizadas en este procedimiento, constituya una infracción directa de la normativa de protección de datos de carácter personal.

Todo ello sin perjuicio del control del efectivo funcionamiento de las garantías y procedimientos de cancelación tomados en consideración en esta resolución que esta Agencia, en el ejercicio de sus funciones, pueda llevar a cabo en el futuro, de oficio o a instancia de los afectados.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

- 1. PROCEDER AL ARCHIVO** de las presentes actuaciones.
- 2. NOTIFICAR** la presente Resolución a GOOGLE INC., a GOOGLE SPAIN, S.L. y a PRIVACIDAD EN INTERNET S.L.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos