



La consulta plantea la conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD), y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RDLOPD) del sistema de grabación de videocámaras a instalar en el interior y exterior de grúas de asistencia en carretera, para dejar constancia de las actividades de los vehículos.

Se plantea por tanto la legalidad de un sistema de videovigilancia en el que la finalidad, si bien expresada muy someramente, estaría constituida porque la empresa de asistencia en carretera justifique el cumplimiento de sus funciones. La finalidad a que se destina el sistema propuesto es esencial para determinar su legitimidad y condiciones de uso, como posteriormente se indicará, por lo que ante la generalidad de los términos de la consulta la respuesta habrá de ser igualmente genérica. Asimismo, la cuestión ha de tratarse diferenciadamente en cuanto a las cámaras a instalar en el interior frente a las del exterior de los vehículos. Comenzaremos estudiando la cuestión que afecta a las cámaras en el interior de los vehículos, cuestión que puede afectar de una manera importante al control de los trabajadores.

I

En primer lugar, los sistemas de videovigilancia suponen un tratamiento de datos de carácter personal. De conformidad con los artículos 1 y 2.1 LOPD, la normativa que nos ocupa tiene por objeto la protección de los datos de carácter personal como derecho fundamental, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*. La imagen de una persona es un dato personal, considerando también el artículo 5.1. f) RDLOPD, que como tales *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*. Y en este mismo sentido el Considerando 14 de la Directiva 95/46/CE que señala *“(14) 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;”.

Por su parte, 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”*. De acuerdo con esta definición de tratamiento de datos personales, la captación y en su caso grabación de imágenes de las personas constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.

En este mismo sentido se pronuncia 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.

Todo tratamiento de datos personales ha de estar legitimado por alguna de las causas del art. 6 LOPD. Pues bien, la captación y grabación de las imágenes de los empleados del centro con un fin de control laboral aparece amparado por el art. 6 LOPD, al existir una habilitación legal para el control laboral pretendido que es de carácter imperativo para *“las partes de un contrato... de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”*.

En el supuesto planteado, la instalación de cámaras en el interior de los vehículos, que captaran las imágenes relativas a los trabajadores de la empresa, a efectos de acreditar la correcta prestación del servicio de asistencia en carretera, parece – teniendo en cuenta los términos genéricos en los que se plantea la consulta – que tendría por finalidad que el empresario controlara el cumplimiento por parte de sus trabajadores de sus obligaciones laborales. Así parece desprenderse de las diversas afirmaciones del consultante, que en un primer momento afirma que la finalidad de estas cámaras es *“grabar al conductor del vehículo”* indicando que *“el material almacenado sólo sería operado en caso de accidente o de alguna infracción laboral”*. Posteriormente se complementa indicando que *“la única finalidad [es] prevenir accidentes y obtener pruebas sobre posibles infracciones de tráfico así como para dar*



mayor seguridad a los trabajadores en su quehacer diario". Entendemos, por tanto, que la finalidad es el control laboral por el empresario de sus trabajadores en cuanto al cumplimiento de sus deberes laborales.

Por tanto, sería de aplicación el artículo 20.3 del Texto Refundido del Estatuto de los Trabajadores (ET), aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre – cuyo tenor literal apenas ha cambiado respecto de la versión anterior en lo que ahora interesa -, dispone que *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad"*.

En este sentido, el artículo 20.3 ET en relación con el art. 6 LOPD legitimaría, en principio, a la consultante como empleadora para tratar las imágenes de los trabajadores en el ámbito laboral con carácter general, sin que fuera necesario el consentimiento de los trabajadores.

Y así lo ha venido reiterando la jurisprudencia en lo que a empleados públicos se refiere amparado en el art. 6.2 LOPD, como en Sentencia de la Sala Tercera del Tribunal Supremo de 2 de julio de 2007 (Rec. 5017/2003) que señala que el control del cumplimiento del horario de trabajo a que vienen obligados los empleados públicos es inherente a la relación que une a estos con la Administración en cuestión, y no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Asimismo, la Sentencia de la misma Sala de 2 de julio de 2007 (Rec. 5017/2003) indica: *"Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos"*.

Ahora bien, esta legitimación no es absoluta y exige que el **empresario informe de dicho tratamiento a los trabajadores** (cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.). Y no sólo a los trabajadores, sino **también a sus representantes**. En este punto resulta ilustrativa y capital la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero, recurso de amparo



10522/2009, cuya conclusión es: *“Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa (...) No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”.*

En este sentido hay que tener en cuenta la Sentencia de la Sala de lo Social del Tribunal Supremo de 13 de mayo de 2014, rec. 1685/2013 en un supuesto de despido de una trabajadora derivado de incumplimientos a través de las imágenes captadas por un sistema de videovigilancia, que dispone lo siguiente: *“por la empresa no se dio información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni, lo que resultaría más trascendente, tampoco se informó, con carácter previo ni posterior a la instalación, a la representación de los trabajadores de las características y alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, ni explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”*

Y así ha venido aplicándose por esta Agencia, como en la Resolución recaída en el PS/00724/2014. En definitiva, el tratamiento de imágenes de los trabajadores con fines de control laboral está admitido con carácter general, al aparecer legitimado por el art. 20.3 ET, en la medida en que cumpla todos los requisitos de la LOPD incluyendo en todo caso la previa información a los trabajadores y a sus representantes.



Sin embargo, ello no implica que en el ámbito laboral quepa todo tratamiento de datos personales para el control por el empresario del cumplimiento de los deberes laborales del trabajador. Es decir, una cosa es la finalidad del tratamiento, que en este caso sería la prevista en el art. 20.3 ET, y otra la necesaria aplicación del principio de proporcionalidad consagrado en el art. 4.1 LOPD únicamente permitiendo el tratamiento de datos *“adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”*.

Respecto de la **proporcionalidad**, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de *“una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad*.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)”.

Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos.

En definitiva, el control laboral como causa legitimadora para el tratamiento de datos personales no implica, *per se*, que quepa todo tratamiento de datos amparado en dicha finalidad. Y en el aspecto que nos ocupa relativo a la videovigilancia, el tratamiento de todas las imágenes que ocupan la jornada laboral de un trabajador, como mecanismo de seguimiento continuo y permanente de su actividad pudiera resultar excesivo al suponer una verdadera



monitorización de los trabajadores, y sin que se ofrezca una causa concreta, temporalmente limitada y ponderada, como podría suceder si existiera un problema concreto con un trabajador determinado relativo al cumplimiento de sus deberes laborales. Se trata de una cuestión ampliamente abordada en diversos documentos internacionales que pasamos a estudiar.

Y es que en el ámbito estrictamente laboral, existen diversos documentos internacionales que abordan la problemática de la protección de datos en dicho ámbito. En el **Grupo de Berlín**, constituido en el seno de la Conferencia Internacional sobre Protección de Datos, el documento **“Informe y Recomendaciones sobre las Telecomunicaciones y la Privacidad en las relaciones laborales” (agosto de 1996)**, ya analiza los riesgos inherentes al control y vigilancia de los empleados a través de las Tecnologías de la Información y de las Comunicaciones, que suponen en muchas ocasiones una intrusión en su privacidad.

En dicho documento se estudian en primer lugar los métodos de recogida de datos más comunes utilizados en el seno de las organizaciones empresariales, tales como los dispositivos magnetofónicos, audio-visuales, transmisores de infrarrojos, identificadores de datos biométricos, dispositivos de videovigilancia, y comunicaciones electrónicas, alertando sobre los riesgos y perjuicios que el uso desviado de dichos medios puede ocasionar al trabajador. Y es que, en lo que ahora interesa, hace especial referencia a los sistemas de videovigilancia, en su caso utilizados en un primer momento con fines de seguridad privada, que graban datos personales de los trabajadores como hábitos de trabajo, relaciones conductuales con los compañeros de trabajo y con terceros no trabajadores en la empresa.

A modo de recomendación, y en orden a garantizar que tal uso será legítimo, necesario, adecuado, pertinente, y proporcionado a la finalidad que lo justifica, se establecen los necesarios controles, en los que se implica muy especialmente a los “representantes de los trabajadores”. Así, tanto los trabajadores como sus representantes, deberán ser informados del tipo de tecnología utilizada por el empresario en relación con la vigilancia y seguimiento de su actividad laboral, debiendo abstenerse el empleador de recoger datos personales que resulten excesivos en razón de la propia naturaleza de la relación laboral. A su vez, los representantes de los trabajadores obtendrán cumplida información sobre la introducción de cualquier nuevo sistema de registro de datos que afecte al conjunto de los trabajadores,

teniendo estos últimos la posibilidad de acceder a los datos que se procesen sobre ellos y el derecho a rectificar los posibles errores que les afecten.

Señala también, que salvo excepciones extremas, fundamentadas en una firme sospecha sobre la existencia de actividades delictivas o dolosas del trabajador, el derecho de Información en la recogida de datos constituye un requisito indispensable para utilizar, en su caso, la información recabada en el lugar de trabajo contra el propio trabajador. En este supuesto, el empleado deberá tener la oportunidad de acceder a la información que le es adversa a fin de poder rebatirla.

Ahora bien, indica el documento en cuestión que las nuevas tecnologías de la información permiten la monitorización continua y la vigilancia en el lugar de trabajo. En determinados casos, la información sobre la actuación o el comportamiento personal de los trabajadores puede ser recopilada y utilizada secretamente para propósitos sobre los que los trabajadores no son conscientes.

Y en este sentido, uno de los parámetros a tomar en cuenta para determinar la proporcionalidad en el tratamiento de los datos son las expectativas razonables y legítimas de privacidad de los trabajadores, que deberán ser analizadas según las circunstancias del caso, sin que en ningún caso el tratamiento pueda ser contrario a su dignidad. Específicamente el informe estudiado afirma que si bien las razones de seguridad permiten que las máquinas sean vigiladas, puede ser excesivo extender la vigilancia a las personas que trabajan con tales máquinas.

Y en este punto es esencial que en ningún caso el empresario pueda tratar datos personales que no sean directamente relevantes en el ámbito de la relación laboral, como el comportamiento o las características personales de los trabajadores o los contactos internos con otros trabajadores o externos del trabajador. Este punto se torna en esencial, puesto que el sistema propuesto supondría la monitorización completa de los trabajadores, de modo que los sistemas de tratamiento de datos permitirían la supervisión de toda su actuación, tanto con los niños del centro de educación infantil como con otros trabajadores, permitiendo un constante seguimiento de su actuación, y excediendo por tanto notoriamente el poder directivo del empresario.

Por su parte, el **Grupo de Trabajo del artículo 29**, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado



en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE 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, en su **Dictamen 8/2001 (WP 48)**, sobre el tratamiento de datos personales en el contexto laboral, parte de la base de que muchas de las actividades realizadas de forma rutinaria en el ámbito de la empresa implican el tratamiento de datos personales de los trabajadores y, en muchas ocasiones, de información de carácter personal especialmente protegida.

Indica el Dictamen 8/2001 que *“La recopilación, almacenamiento y uso de información sobre los trabajadores por medios electrónicos, y las diversas herramientas de uso común en buena parte de las empresas, tales como el correo electrónico o el acceso a Internet, implican en muchas ocasiones el tratamiento de datos personales de los trabajadores. A ello se unen otras nuevas modalidades de control del trabajador, que llegan de la mano de la imagen y el sonido, entre las que destacan los sistemas de videovigilancia a los que se debe aplicar la normativa sobre protección de datos.”*

En el citado Dictamen, el Grupo enumera y desarrolla los Principios Fundamentales de la Protección de Datos, que los empresarios deberán tener siempre en cuenta en el contexto laboral. Así, los principios de Finalidad y de Transparencia, referidos a la necesidad del uso legítimo de los datos, adecuados a un fin determinado y explícito, propio de la actividad laboral, y a la necesidad de que los trabajadores conozcan qué datos recoge el empresario sobre ellos. Según se apunta en el Dictamen, la Transparencia también podría garantizarse otorgando al interesado el derecho de acceso a los datos personales que les afectan. De este modo, los trabajadores, como partes interesadas en la relación laboral, deben beneficiarse de los derechos que confiere la Directiva sobre protección de datos y, muy especialmente, del derecho de acceso, previsto en el artículo 12 de la misma.

El principio de legitimidad se vincula al de proporcionalidad, debiendo ser los datos recabados, adecuados, pertinentes y no excesivos en relación con la necesidad de su recogida, y disponiéndose la necesidad de que los trabajadores sean suficientemente informados sobre la existencia de dicho tratamiento legítimo y proporcionado. Así, en lo referente a la vigilancia de los trabajadores a través del correo electrónico, Internet, cámaras de vídeo o datos de localización, el control deberá ser una respuesta proporcionada del empresario ante riesgos potenciales, teniendo en cuenta el derecho a la vida privada y otros intereses de los trabajadores.



Y en lo que ahora interesa el dictamen contiene un apartado específicamente destinado a vigilancia y monitorización (apartado 12), mencionando específicamente el uso de videovigilancia. Afirma el texto que (la traducción es nuestra) *“cualquier monitorización debe ser una respuesta proporcionada de un empresario a los riesgos a los que se enfrente, considerando la legítima privacidad y otros intereses de los trabajadores. Cualquier dato personal conservado o utilizado en el seno de una monitorización ha de ser adecuado, pertinente y no excesivo para la finalidad perseguida. Cualquier monitorización ha de ser llevada a cabo del modo menos intrusivo posible”*. Y se enfatiza siempre en la necesidad de establecimiento de una medida proporcionada y lo menos intrusiva posible en la privacidad de los trabajadores.

De nuevo, este documento da respuesta a la cuestión estudiada, por cuanto el sistema planteado prevé, sin distinción, una monitorización de toda la actividad de los trabajadores. Otra cosa sería que se hubiera planteado el uso del sistema ante una situación concreta y particular de importantes incumplimientos concretos de deberes laborales, o únicamente durante pequeños periodos de tiempo o por motivos determinados que hicieran proporcional el uso del sistema. Ahora bien, la implantación de un sistema de videovigilancia de monitorización permanente de los trabajadores, además de ser excesivo por poder conseguirse las finalidades a través de mecanismos menos intrusivos, supondría un control que excedería del poder directivo, permitiendo el control de todos y cada uno de los comportamientos de los trabajadores, sin mencionar ningún riesgo potencial en particular, y suponiendo una importantísima intervención en la vida privada de los trabajadores. Una cosa es la tolerancia por los trabajadores de un determinado grado de intrusión en su privacidad, como parte de una organización empresarial, y otra distinta el uso ilimitado de estos mecanismos que podría atentar contra la dignidad de los trabajadores.

Si bien entendemos que la cuestión de la monitorización y la vigilancia permanente de los trabajadores ha quedado suficientemente estudiada, también puede mencionarse el **Documento de Trabajo del Grupo del Artículo 29, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo de 29 de mayo de 2002 (WP 55)**, en el que se examina la vigilancia por el empleador de la utilización del correo electrónico e Internet por parte de los trabajadores, ofreciendo una orientación y ejemplos concretos

sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empresario.

Cabe destacar que dicho Documento de Trabajo señala respecto del principio de proporcionalidad que *“Según este principio, los datos personales, incluidos los que se utilicen en las actividades de control, deberán ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben. La política de la empresa en este ámbito deberá adaptarse al tipo y grado de riesgo al que se enfrente dicha empresa.*

El principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua).”

Más recientemente la **Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa de 1 de abril de 2015 sobre el tratamiento de datos en el ámbito laboral**, partiendo la necesaria minimización de los riesgos para la privacidad de los empleados considerando los actuales métodos de tratamiento de datos derivados del uso de nuevas tecnologías, establece una serie de principios aplicables, según su artículo 1, al tratamiento de datos personales de los empleados en los sectores público y privado. En concreto, el artículo 15 contempla los sistemas de información y tecnologías para la monitorización de empleados, incluyendo videovigilancia. Y se recomienda que no se permitan estos sistemas y tecnologías cuando su finalidad *“directa y principal sea la monitorización de la actividad y comportamiento de los empleados”* (la traducción es nuestra). Únicamente se contempla su posible utilización, y siempre con las debidas salvaguardas, incluida la previa consulta de los representantes de los trabajadores, cuando sean empleados con otra finalidad y su consecuencia indirecta sea la posibilidad de tal monitorización. Asimismo se prevé en el apartado 15.2 que en tales supuestos los sistemas y tecnologías sean *“específicamente diseñados y situados de forma que no socaven sus derechos fundamentales. El uso de videovigilancia para la monitorización de ubicaciones que son parte del área más personal de la vida de los empleados no está permitido en ninguna situación”*.



En definitiva, en ningún caso la instalación de un sistema de videovigilancia que permita un seguimiento continuo de la actividad de los trabajadores de una empresa de asistencia en carretera monitorizando su actividad laboral puede entenderse ajustado al principio de proporcionalidad debido a la intromisión en la vida privada que ello representa, al carácter amplio e ilimitado del sistema y a la posible utilización de otros medios alternativos que permitieran la consecución de los fines perseguidos según la consulta. En lo que atañe a la vida privada no podemos dejar de mencionar la **Sentencia del Tribunal Europeo de Derechos Humanos de 23 de noviembre de 1992, caso Niemitz contra Alemania**, en la que se indicó (apartado 29): *“El Tribunal no considera ni posible ni necesario buscar la definición exhaustiva de la noción de “vida privada”. No obstante, sería demasiado restrictivo limitarla a un “círculo íntimo” donde cada uno puede llevar su vida personal como quiera, y separarla totalmente del mundo exterior a este círculo. El respeto a la vida privada debe incluir también, en cierta medida, el derecho de los individuos para establecer y desarrollar relaciones con sus semejantes.*

Parece, además, que no existe ninguna razón de principio para considerar esta forma de entender el concepto de “vida privada” como excluyendo las actividades comerciales o profesionales: después de todo, es en su trabajo donde la mayoría de las personas tiene muchas, incluso la mayoría de oportunidades para fortalecer sus vínculos con el mundo exterior. Un hecho señalado por la Comisión, lo confirma: en la actividad profesional de alguien, no siempre se puede desentrañar lo que entra dentro del ámbito profesional de lo que no. En especial, las tareas de un miembro de una profesión liberal pueden constituir un elemento de su vida en grado tan alto, que no podía decir en qué condición se encuentra en un momento dado”.

Y también en este sentido la **Sentencia del mismo tribunal, Sección 3ª de 24 junio 2004 Asunto Von Hannover contra Alemania** señala: *“Además, la esfera de la vida privada, tal como la concibe el Tribunal, cubre la integridad física y moral de una persona; la garantía que ofrece el artículo 8 del Convenio está destinada principalmente a asegurar el desarrollo, sin injerencias externas, de la personalidad de cada individuo en la relación con sus semejantes (...)*

El Tribunal ha señalado igualmente que, en ciertas circunstancias, una persona dispone de una «esperanza legítima» de protección y de respeto de su vida privada”.

En conclusión, no cabe la instalación de un sistema de videovigilancia que, con carácter permanente y no discriminando situaciones concretas, implicara la captación y grabación de las imágenes de los trabajadores en el interior de los vehículos. Otra cosa sería que el sistema se implantara específicamente en determinados momentos o casos en que pudiera plantearse un presunto incumplimiento concreto y particular de un determinado trabajador o grupo de trabajadores; o bien que el sistema se concibiera de tal modo que sólo se activara la grabación ante determinados eventos, como puede ser un posible accidente de circulación, o en determinados casos.

II

En segundo lugar, se plantea la cuestión relativa a la implantación del sistema de videovigilancia en el exterior de los vehículos. En este caso no se indica concretamente la finalidad perseguida. En un primer momento la consulta señala que la finalidad es *“grabar todo lo que acontece delante del vehículo en un ángulo de 180 grados”* y posteriormente se indica la finalidad ya expresada anteriormente de *“prevenir accidentes y obtener pruebas sobre posibles infracciones de tráfico así como para dar mayor seguridad a los trabajadores en su quehacer diario”*, sin distinguir si esta es la finalidad perseguida para las cámaras interiores o bien para las que se pretenden instalar en el exterior de los vehículos. Como decíamos anteriormente, la delimitación de la finalidad del sistema es esencial.

Y es que en lo que respecta a la legitimación para el tratamiento de los datos, en cuanto a las cámaras a instalar en el exterior de los vehículos, el tratamiento se podría encontrar amparado por el **interés legítimo** regulado en el artículo 7.f) de la Directiva 95/46/CE.

En cuanto a esta legitimación amparada en el artículo 7.f) de la Directiva 95/46/CE debe traerse a colación lo ya indicado por esta Agencia en su informe de 12 de marzo de 2012 en el que se indicaba lo siguiente:

“El marco normativo en materia de protección de datos se ha visto sensiblemente afectado por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en el seno de los recursos interpuestos por diversas asociaciones, entre ellas la propia consultante, contra

el Reglamento de desarrollo de la Ley Orgánica 15/1999. A su vez, el marco se ve igualmente afectado por las Sentencias dictadas por el Tribunal Supremo en fecha 8 de febrero de 2012, por las que se resuelven los mencionados recursos.

La Sentencia del Tribunal de Justicia ha declarado expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) 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”. 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”.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, 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,



conforme a su apartado 47 que “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”.

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existe un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado 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.

En el presente caso, el interés legítimo alegado no está claro. Por un lado parece que se encontraría relacionado con el control laboral pero por otro lado parece referirse especialmente al derecho fundamental a la tutela judicial efectiva (art. 24 CE), en la medida en que las imágenes grabadas únicamente se utilizarán para la obtención de pruebas con la finalidad de determinar las responsabilidades asociadas a la producción de un evento, es decir, *“obtener pruebas sobre posibles infracciones de tráfico”*.

El alcance del derecho a la tutela judicial en relación con la prueba ha sido abordado, entre otras, en la STC 212/2013, de 16 de diciembre, en la que se hace referencia, citando la STC 88/2014, de 28 de mayo a *“las íntimas relaciones del derecho a la prueba con otros derechos garantizados en el art. 24 CE. Concretamente, en nuestra doctrina constitucional hemos hecho hincapié en la conexión de este específico derecho constitucional con el derecho a la tutela judicial efectiva (art. 24.1 CE), cuyo alcance incluye las cuestiones relativas a la prueba (SSTC 89/1986, de 1 de julio, FJ 2; 50/1988, de 22 de marzo, FJ 3; 110/1995, de 4 de julio, FJ 4; 189/1996, de 25 de noviembre, FJ 3; y 221/1998, de 24 de noviembre, FJ 3), y con el derecho de defensa (art. 24.2 CE), del que es inseparable (SSTC 131/1995, de 11 de septiembre, FJ 2; 1/1996, de 15 de enero, FJ 2; y 26/2000, de 31 de enero, FJ 2)” (STC 19/2001, de 29 de enero, FJ 4; y, en el mismo sentido, STC 133/2003, de 30 de junio, FJ 3)»*. En las reseñadas SSTC 19/2001 y 133/2003 el Tribunal Constitucional apuntaba que *“ha sido justamente esta inescindible conexión (con los otros derechos fundamentales mencionados, en particular el derecho a obtener una tutela judicial efectiva), la que ha permitido afirmar que el*

contenido esencial del derecho a utilizar los medios de prueba pertinentes se integra por el poder jurídico que se reconoce a quien interviene como litigante en un proceso de provocar la actividad procesal necesaria para lograr la convicción del órgano judicial sobre la existencia o inexistencia de los hechos relevantes para la decisión del conflicto objeto del proceso (por todas, STC 37/2000, de 14 de febrero, FJ 3)”.

La relación entre los derechos a la protección de datos personales y a la tutela judicial ha sido, asimismo, analizada en el Informe 469/2011 de 30 de diciembre de 2011, en el que se indica lo siguiente:

“En este punto, debe recordarse que esta Agencia ya ha tenido la ocasión de analizar la posible concurrencia en un determinado supuesto de tratamiento de datos de los derechos fundamentales a la protección de datos de carácter personal y a la tutela judicial efectiva del responsable del tratamiento. Así, se ha considerado por ejemplo que el tratamiento por un abogado de los datos de la parte contraria de su cliente encuentra su amparo en el reconocimiento a éste último por el artículo 24.1 de la Constitución de su derecho a la tutela judicial efectiva, lo que implica, según el apartado 2, la defensa letrada y el uso de los medios de prueba pertinentes para la defensa de su derecho. En este sentido, el informe de 21 de febrero de 2001 se señalaba lo siguiente:

“En este caso, como se dijo, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquéllos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 del Texto Constitucional.

En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que su cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la posibilidad de aportación por el interesado de “los medios de prueba pertinentes para su defensa”, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Por todo ello, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de



los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los Órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes.

Por todo ello, existe, desde nuestro punto de vista, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 de la Constitución y sus normas de desarrollo.”

El informe concluye afirmando que, en principio, sería posible entender que el tratamiento y la cesión de datos podrían entenderse amparadas y legitimadas en los artículos 6.11 y 11.2.a) de la LOPD, en conexión con el artículo 24 de la Constitución, siempre que se cumplan las garantías aportadas.

El citado informe analiza también la conexión entre esta última conclusión y la legitimación amparada en el artículo 7.f) de la Directiva 95/46/CE, reiterando al necesidad de ponderar si el derecho a la tutela judicial efectiva y a la defensa alegados por la consultante prevalecen o no sobre el derecho a la protección de los datos personales.

Partiendo de estas premisas, procede, por tanto, llevar a cabo esta ponderación atendiendo a las circunstancias específicas del caso al que se refiere la consulta. Para ello, deberán tenerse en cuenta, adicionalmente, las previsiones de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de seguridad en lugares públicos.

La norma citada atribuye a las Fuerzas y Cuerpos de Seguridad la competencia exclusiva para la instalación de videocámaras fijas o móviles en lugares públicos, circunstancia que concurre en la presente consulta, al menos, respecto de la captación de imágenes hacia el exterior del vehículo de transporte.

Así se ha reconocido en numerosas resoluciones de la Agencia, entre las que cabe citar la del E/00223/2013, en la que se afirma lo siguiente:



“Primeramente, respecto a la posible captación por parte de la entidad denunciada, a través de su sistema de videovigilancia, de imágenes de la vía pública, hay que señalar que para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: “La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública”.

Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) de la Ley Orgánica 15/1999, donde se prevé que: “Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia”.

En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, señalándose en su artículo 2.2, en lo que hace mención a su ámbito de aplicación que *“Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal.”*

No obstante, la misma resolución admite una legitimación limitada para la captación de imágenes en la vía pública siempre que se garantice el cumplimiento del principio de proporcionalidad regulado en el artículo 4.1 y 2 de la LOPD, que establece lo siguiente: *“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán*



usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.

En relación con la captación de imágenes con fines de videovigilancia, dicho principio se refleja en el artículo 4 de la Instrucción 1/2006, de 8 de noviembre, con el siguiente tenor literal: *“Principios de calidad, proporcionalidad y finalidad del tratamiento. 1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras. 2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal. 3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida”.*

Si bien el artículo transcrito está relacionado con una finalidad, como es la videovigilancia por razones de seguridad, distinta de la que es objeto de la consulta; también en este caso será preciso garantizar específicamente el cumplimiento del principio de proporcionalidad.

A los efectos de ponderar la prevalencia o no del interés legítimo alegado, y, en particular, la garantía del principio de proporcionalidad, han de valorarse las garantías propuestas para la captación y uso posterior de las imágenes. Ahora bien, en el caso planteado no se proponen garantías de ningún tipo que pudieran ponderarse en los términos expuestos, por lo que sin limitaciones de ningún tipo debemos concluir que no cabe la implantación genérica, y sin límites, de la captación y grabación de imágenes.

Por si fuera de alguna utilidad, podemos referirnos al informe de esta Agencia de 13 de abril de 2015 – complementado por los dos informes de 4 de agosto del mismo año, en sentido idéntico – en el que se planteaba la utilización de cámaras en el frontal de vehículos con la finalidad de obtener

pruebas para el caso en que se produjera un siniestro de tráfico. En dicho informe se concluyó favorablemente, considerando las específicas cautelas implantadas en el sistema en cuestión: como primer punto destacamos que el sistema de grabación únicamente se activaba en caso de producirse un evento concreto, lo que determinaría el posible acaecimiento de un siniestro, o bien la activación manual, como podría plantearse en la consulta que ahora nos ocupa al hablar de *“dar mayor seguridad a los trabajadores en su quehacer diario”*. Dicho informe se pronunciaba en los siguientes términos:

“La finalidad del tratamiento resulta legítima teniendo en cuenta su vinculación con el derecho a la tutela judicial, quedando excluido el uso de las imágenes para otros fines como el control laboral, así como la grabación del sonido en el interior del vehículo que quedará desactivado en su comercialización en España.

La vinculación al derecho a la tutela judicial se concreta en el hecho de que sólo se accederá a las imágenes cuando tenga lugar un evento que se identifica con accidentes o situaciones de peligro en el interior del vehículo, susceptible de generar responsabilidades en el ámbito jurisdiccional.

La comercialización del dispositivo queda limitada a medios de transporte públicos y privados concesionarios de licencias para el transporte de personas y/o mercancías quedando excluida su instalación en otro tipo de vehículos.

La captación de imágenes hacia el exterior queda limitado al frontal del vehículo y, hacia el interior, excluye la captación de la imagen del conductor.

Adicionalmente, las grabaciones efectuadas se cancelan progresivamente pudiendo recuperarse sólo en el caso de producirse un evento. En tal caso la recuperación de las grabaciones queda limitada a un periodo de tiempo máximo de 20 segundos anteriores y posteriores al momento del evento.

El acceso a los videos grabados se restringe a personas específicamente autorizadas con credenciales específicas y cuentas dedicadas.

En el tratamiento de las imágenes después de producirse el evento, se difuminarán las de las personas u otros datos como matrículas que no estén involucradas en el mismo.

El conjunto de restricciones que se han descrito permite minimizar el tratamiento de los datos personales quedando limitado a los datos adecuados, pertinentes y no excesivos en relación con la finalidad para la que se obtuvieron.

En cuanto a la conservación de los datos, el dispositivo permite un registro máximo de 300 eventos cancelándose automáticamente por orden de antigüedad una vez que se haya alcanzado dicho límite. No obstante, se prevé un plazo temporal de conservación de las imágenes por un periodo máximo de tres años, que se justifica por ser el plazo de prescripción de las infracciones muy graves reguladas en la LOPD.

Alternativamente se contempla la posibilidad de que dicho plazo sea el de un año previsto en el artículo 1968 del Código civil para la prescripción de acciones.

En este punto la decisión del Garante a que antes se hizo referencia vincula la conservación de las imágenes con los plazos de prescripción de las acciones legales frente a la producción de los daños causados como consecuencia del evento; criterio que cumple con mayor rigor el principio de proporcionalidad respecto de la finalidad declarada de posibilitar la obtención de pruebas en el ejercicio del derecho a la tutela judicial. Lo que no obsta a la conservación por un plazo superior de aquellas imágenes directamente vinculadas a una investigación policial o un procedimiento ya iniciados.

Las medidas de seguridad propuestas para el tratamiento de los datos son los que el artículo 81 y concordantes del RLOP califica como de nivel medio, criterio que puede vincularse al hecho de que, en ocasiones, las imágenes estarán relacionadas con la comisión de infracciones administrativas o penales.

Respecto de la transparencia en el tratamiento de los datos, es decir, de la información que ha de facilitarse a los interesados, la consulta describe un abanico de opciones que se complementan entre sí, e incluyen un cartel visible en el interior del vehículo, la incorporación de cláusulas informativas en la documentación dirigida a los pasajeros y en la página web del responsable del

tratamiento o, en su caso, de sus perfiles sociales. A los que se añade la realización de una campaña informativa por parte de los responsables del tratamiento sobre el uso y las funcionalidades del dispositivo previa al tratamiento de los datos a través de sus servicios de atención al cliente. El conjunto de opciones propuestas permitirían, por tanto, garantizar que los interesados puedan obtener la información requerida por el artículo 5 de la LOPD. En particular, la campaña informativa a través de los servicios de atención al cliente coincide con la recomendación que en idéntico sentido incluyo la decisión del Garante antes citada.

No obstante, se excluye la información sobre las cesiones a jueces y a la policía estando esta última excluida entre las previstas en el artículo 11.2. d) de la LOPD, por lo que debería completarse la información.

Sobre la información para el tratamiento de datos en el exterior del vehículo no se indica una fórmula específica, si bien cabría admitir un procedimiento simplificado análogo al contemplado en la Instrucción 1/2006, de 8 de noviembre, consistente en un pictograma o dibujo de fácil comprensión sobre la finalidad del tratamiento y el responsable ante el que pueden ejercitarse los derechos ARCO.

Dicha información debería completarse implantando procedimientos para poner a disposición de los interesados el resto de los extremos recogidos en el artículo 5 de la LOPD.

Teniendo en cuenta cuanto se acaba de indicar, aplicada la regla de ponderación exigida por el TJUE al objeto de la consulta, cabe concluir que los tratamientos de datos, siempre que cumplan todas las garantías que se han descrito, se encuentran amparadas en el artículo 7.f) de la Directiva 95/46/CE en conexión con el artículo 24 de la Constitución”.