



Expediente N°: E/00488/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CARREFOUR NORTE, S.L.** y **SEGURIDAD PRIVADA SEGURIBER S.L.U.** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 27 de noviembre de 2013 tiene entrada en esta Agencia escrito de D. **A.A.A.** (en adelante el denunciante), vigilante de seguridad de la empresa **SEGURIDAD PRIVADA SEGURIBER S.L.U.** (en adelante el denunciado), comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la utilización de las cámaras de videovigilancia cuyo titular es la entidad **CARREFOUR NORTE, S.L.** instaladas en "**CARREFOUR ERANDIO**" ubicado en (C/.....1) (**VIZCAYA**).

El denunciante manifiesta que la empresa **SEGURIBER, SLU**, en fecha 8 de agosto de 2012 le notifica carta de sanción, acusándole de unos hechos acaecidos el día 6 de julio de 2012 que han sido grabados por las cámaras de videovigilancia y aportadas por la empresa **SEGURIBER** en un DVD como prueba de una sanción disciplinaria de falta muy grave impuesta al denunciante.

Aporta copia de la sentencia nº ****/2013 del Juzgado de lo Social nº 10 de Bilbao, de fecha 22 de octubre de 2013, revocatoria de la sanción impuesta al denunciante.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

-Con fecha 21 de febrero y 3 de julio de 2014 se solicita información a **CARREFOUR NORTE, S.L.** como responsable del establecimiento teniendo entrada en esta Agencia con fecha 12 de marzo y 1 de agosto de 2014 dos escritos del representante legal en los que manifiesta:

1. Tener la representación otorgada, para ello aporta copia de la escritura de poder, otorgado por "**CARREFOUR NORTE, S.L.**"
2. El responsable de la instalación es Carrefour Norte, S.L. con NIF B48609069 con domicilio en Cr. de Baracaldo-San Salvador del Valle, Polígono Ibarzaharra (nave 2), 48510 Sestao (Vizcaya). Aporta copia del fichero de titularidad privada inscrito en esta Agencia como Doc 1 y 3.
3. Aporta como Doc. 2 copia del Acuerdo de prestación de servicios de seguridad firmado entre otros centros de Carrefour, por **Carrefour Norte, S.L.** y **SENSORMATIC ELECTRONICS CORPORATION SERVICIOS, S.A.**, (homologada por el Ministerio del Interior con el nº *****) para el suministro, instalación y servicio de mantenimiento de dispositivos y sistemas de circuitos cerrados de televisión (CCTV) con fecha 7 de abril de 2011, cuyo anexo III es la copia del acuse de recepción y certificado de instalación. Aporta el cambio de denominación de **SENSORMATIC ELECTRONICS CORPORATION**

SERVICIOS, S.A a TYCO INTEGRATED FIRE AND SECURITY CORPORATION SERVICIOS acordada por la DGP con fecha 3/6/2013.

4. El motivo de la instalación de las cámaras es: la captación, grabación y almacenamiento de imágenes obtenidas a través de los sistemas de videovigilancia de la sociedad.
5. Adjunta varias fotografías de carteles informativos ubicados en puntos de entrada al garaje y al aparcamiento al aire libre de las instalaciones con indicación del responsable (y la dirección) ante el que ejercitar los derechos de la LOPD: **CARREFOUR NORTE, S.L.**, Apartado de Correos 1002, C.P. 28108, Alcobendas, Madrid. Se adjunta como Doc. 4.
6. Adjunta modelo del formulario informativo con indicación de los datos del responsable del fichero, en español y euskera como Doc 5.
7. Adjunta listado y plano de situación con ubicación de las cámaras instaladas tanto en el interior del local como en aparcamiento, como Doc. 6.
8. Aporta fotografía de todas las cámaras instaladas y de las imágenes captadas como Doc. 7.
9. Aporta fotografía de tres monitores que visualizan las imágenes captadas como Doc. 8.
10. El personal que accede al sistema de videovigilancia es: el jefe de Servicios del centro y los vigilantes del centro (Seguridad Castellana). Aporta como Doc. 9 copia de la Adenda al Contrato de Prestación de Servicios de Vigilancia entre Grupo Carrefour y Castellana de Seguridad, S.A.U. de fecha 15 de enero de 2012, donde aparece incluido el centro **CARREFOUR NORTE, S.L.** además de documentación de procedimiento de prevención.
11. Aporta copia del documento de seguridad del fichero de videovigilancia de nivel básico como Doc. 10.
12. El sistema está conectado a una central de alarmas. Aporta copia de certificado de conexión a la empresa **PYCSECA**, de fecha 3/3/2014, con nº 914 en el Registro de Empresas de Seguridad de la DG de Seguridad del Estado, copia de la prórroga del contrato suscrito el 20/12/2011 firmada a 20/12/2012, copia del contrato de instalación y mantenimiento de la CRA de 20/12/2011 donde se incluye, entre otros centros, el de **CARREFOUR NORTE, S.L.**, junto con un procedimiento de prevención, como **Doc. 11.1.**

Aporta copia de la documentación que acredita a **TYCO INTEGRATED FIRE AND SECURITY CORPORATION SERVICIOS** ante la DGP con nº ***** en fecha 25/6/2013 como Doc. 11.2 y 11.3

-Con fecha 4 de julio de 2014 se solicita la siguiente información a **SEGURIBER**:

- Detalle de las personas que pueden acceder al sistema de videovigilancia instalado. Adjuntar copia del contrato de **SEGURIBER** con **CARREFOUR** correspondiente a 2012.
- Detallar el procedimiento empleado para informar a los trabajadores de la finalidad por la cual se han instalado las cámaras de videovigilancia y adjuntar la documentación acreditativa del cumplimiento del citado procedimiento.

- Aportar las imágenes presentadas como prueba en el auto 807/2012 en el Juzgado de lo Social nº 10 de Bilbao con sentencia ****/2013 de 22/10/2013.

Con fecha 18 de julio de 2014 tiene entrada en esta Agencia escrito del denunciado en el que manifiesta:

En contestación al escrito de 4 de los corrientes, [...] Ref. E/00488/2014, por el que se solicita determinada documentación e información en relación al sistema de videovigilancia instalado en CARRREFOUR ERANDIO, sito en la (C/.....1), de la localidad de ERANDIO (VIZCAYA), parece oportuno significar que la empresa de seguridad Securiber, S.L.U. no presta servicio en las mencionadas instalaciones desde el día 1 de septiembre de 2012, en que quedó resuelta la relación contractual que mantenía con la compañía titular de las instalaciones.

Se adjunta como se interesa, copia del contrato de fecha 15 de enero de 2012, suscrito en su momento entre esta compañía de seguridad y distintas sociedades del Grupo Carrefour.

En el contrato que entró en vigor el 1 de febrero de 2012, figura el centro **Carrefour Norte, S.L.**, cuyo objeto, entre otros, es la vigilancia y protección de las instalaciones, siendo la EMPRESA Securiber.

En el apartado V. Características del servicio que se contrata, se indica que:

“V.1. El Servicio se prestará mediante Vigilante de Seguridad, con instrucción suficiente y formación continuada, cuya impartición será responsabilidad de LA EMPRESA, en relación con sus derechos, deberes y responsabilidades como Vigilantes de Seguridad, así como sobre sistemas de vigilancia, control de accesos, sistemas de alarma y otros relativos o que pudieran afectar al servicio prestado.”

En el apartado VII. Situación Laboral se indica que:

“VII.1. Los Vigilantes de Seguridad prestarán el servicio bajo la dirección y disciplina de LA EMPRESA, en cuya organización se hallan integrados”.

Se incluye la lista de centros amparados por el contrato en el que figura el centro **Carrefour Norte, S.L.**, ubicado en ERANDIO (Vizcaya), el Anexo II con el Pliego de Condiciones (operativa) de Vigilancia de noviembre de 2011, el procedimiento para la coordinación de actividades empresariales en materia de prevención de Carrefour de 28 de enero de 2009.

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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

Con carácter previo, procede situar la materia de videovigilancia en su contexto normativo.

Así el artículo 1 de la LOPD dispone: “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”

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“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”,* 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”*.

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”*.

El artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*.

En este mismo sentido se pronuncia el artículo 2.a) 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, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de esta 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.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”*. Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”*.

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.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.” (el subrayado es de la Agencia Española de Protección de Datos).

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”

De lo anteriormente expuesto 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, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

III

En el presente expediente el D. **A.A.A.**, vigilante de seguridad de la empresa **SEGURIDAD PRIVADA SEGURIBER S.L.U.**, comunica posible infracción a la Ley Orgánica 15/1999 motivada por la utilización de las cámaras de videovigilancia cuyo titular es la entidad **CARREFOUR NORTE, S.L.** instaladas en **"CARREFOUR ERANDIO"** ubicado en **(C/.....1) (VIZCAYA)**, y parte de cuyas imágenes grabadas el día 6 de julio de 2012 fueron aportadas por la empresa **SEGURIBER** en un DVD como prueba de una sanción disciplinaria de falta muy grave impuesta al denunciante.

Pues bien, el artículo 6.1 de la LOPD dispone lo siguiente:

“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. (El subrayado es de esta Agencia)

Por su parte, el apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en el 6.1, estableciendo que *“2. 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 negocial, 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.”*

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, establece, entre otros requisitos, la necesidad de legitimación para que el tratamiento de los datos de carácter personal sea lícito, y así lo dispone el artículo 2 de la citada Instrucción, anteriormente transcrito.

Prima facie, el tratamiento de imágenes por razones de seguridad se encuentra amparado, en el artículo 5.1 e) de la Ley 23/1992, de 30 de julio, de Seguridad Privada, que establece *“1. Con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollen, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades: a) Vigilancia y protección de bienes, establecimientos, espectáculos, certámenes o convenciones, b) Protección de personas determinadas, previa la autorización correspondiente, c) Depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen, o por su peligrosidad, puedan requerir protección especial, sin perjuicio de las actividades propias de las entidades financieras, d) Transporte y distribución de los objetos a que se refiere el apartado anterior a través de los distintos medios, realizándolos, en su caso, mediante vehículos cuyas características serán determinadas por el Ministerio del Interior, de forma que no puedan confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad, e) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, de conformidad con lo dispuesto en la Disposición adicional sexta, f) Explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las Fuerzas y Cuerpos de Seguridad, así como prestación*

de servicios de respuesta cuya realización no sea de la competencia de dichas Fuerzas y Cuerpos, g) Planificación y asesoramiento de las actividades de seguridad contempladas en esta Ley”.

La existencia de cámaras de seguridad en el establecimiento comercial responde a su necesidad e idoneidad para garantizar la seguridad y protección de las instalaciones, bienes y personas, siendo fundamental tanto las cámaras como el servicio que prestan las personas encargadas de visionar las mismas. El tratamiento de las imágenes tanto activo (grabando todo lo que ocurre en las instalaciones) como pasivo (siendo grabado dentro de las instalaciones) de las imágenes, es un elemento inherente a la condición de vigilante de seguridad.

La finalidad del tratamiento de las imágenes, como se ya se ha recogido, es la seguridad de las instalaciones y bienes, pero parte esencial de esta seguridad es el cumplimiento de las obligaciones del personal a cargo de la empresa de seguridad contratada al respecto.

A este respecto, en el contrato de vigilancia y protección que tuvieron en vigor desde el 1 de febrero de 2012 hasta su resolución, entre **CARREFOUR y SEGURIBER**, se recogía en el apartado V. Características del servicio que se contrata, lo siguiente:

“V.1. El Servicio se prestará mediante Vigilante de Seguridad, con instrucción suficiente y formación continuada, cuya impartición será responsabilidad de LA EMPRESA, en relación con sus derechos, deberes y responsabilidades como Vigilantes de Seguridad, así como sobre sistemas de vigilancia, control de accesos, sistemas de alarma y otros relativos o que pudieran afectar al servicio prestado.”

En el apartado VII. Situación Laboral se indica que:

“VII.1. Los Vigilantes de Seguridad prestarán el servicio bajo la dirección y disciplina de LA EMPRESA, en cuya organización se hallan integrados”.

IV

Debe tenerse en cuenta que, en el presente caso lo que procede examinar no es la utilización del sistema de videovigilancia de **CARREFOUR** para el control laboral del denunciante, sino el hecho de que la imagen del denunciante, como trabajador de la empresa de seguridad que presta su servicios a **CARREFOUR**, fuera objeto de captación, grabación y tratamiento en el marco del sistema de videovigilancia implantado por **CARREFOUR** con fines de seguridad.

A este respecto, según recoge el Hecho Probado Segundo de la Sentencia Nº ****/2013 de 22 de octubre de 2013, aportada por el denunciante en la que se revoca la sanción impuesta al mismo recoge: *“El departamento de RRHH ha tenido conocimiento, de una serie de hechos ocurridos en el servicio de seguridad y vigilancia de Carrefour, concretamente en el centro de Erandio. Los sucesos a los que nos referimos han sido transmitidos por el Dpto. Operativo, mediante informe elaborado al efecto. Una vez analizados los mismos, tanto su gravedad como la repercusión que los mismos han*

tenido, ya que los mismos han causado un daño irreparable a la empresa, el departamento de RRHH se ve en la necesidad de tomar las medidas disciplinarias que seguidamente se detallan(...)

Hay que indicar que los hechos expuestos se encuentran registrados en las grabaciones de las cámaras de seguridad de Carrefour.

De la información, obrante en el Dpto. de RRHH de la Empresa, se deduce que la actuación llevada a cabo por usted no fue la que se debía esperar de un vigilante de seguridad, ya que como profesional de la seguridad y con formación suficiente, usted no debería dar este tipo de información a personas ajenas al servicio. Esta información es confidencial y de máxima seguridad y la misma puede ser utilizada para fines delictivos. Los hechos que aquí nos ocupan ocasionan un gran desprestigio a nuestra empresa ante nuestro Cliente Carrefour, al cual se le debe la prestación de los servicios de forma idónea, que no es más que los que se derivan de la relación mercantil y ponen en duda la capacidad para desarrollar las funciones encomendadas, tanto a nuestra empresa como por extensión a los trabajadores de la misma" (...)

Debe significarse que los hechos captados por las cámaras y que derivaron en efectos laborales, se relacionan con cuestiones de seguridad imputadas al denunciado y captadas supuestamente por las cámaras. Al denunciante se le imputa según recoge la propia sentencia que "El día 6 de julio del presente año, usted tenía asignado turno asignado de 15:00 a 22:30 horas, en el Carrefour sito en la localidad de Erandio. Alrededor de las 15.25, se presenta en el Centro de Control de dicho servicio un delegado de CCOO, el cual no es trabajador de esta empresa (...) El problema radica en que usted expone claramente con hechos, como se cierra el centro y todo el protocolo que esto conlleva, para lo cual incluso llega a entrar en el despacho del Jefe de Patrimonio. Por tanto usted da información confidencial a personas ajenas, tanto al cliente como al servicio de seguridad. No se limita a relatar unos hechos, sino que da información pormenorizada de cómo se cierra el centro, de donde se guarda la llave del mismo, como se precinta la llave..."

Hay que indicar que los hechos expuestos se encuentran registrados en las grabaciones de las cámaras de seguridad de Carrefour".

Por lo tanto se le imputaba al denunciante una revelación de protocolo de cierre del centro comercial si bien en el fallo de la sentencia dictada se revocaba la sanción impuesta al denunciante por la empresa de seguridad, al considerarse que no se habían acreditado los hechos objeto de sanción.

Así, el sistema de videovigilancia instalado en **CARREFOUR** tiene por objeto la seguridad y no el control laboral de los trabajadores.

EL seguimiento y utilización de las imágenes de las videocámaras se produjo para fines de seguridad, detectando a través de las mismas un problema de seguridad provocado por el denunciante en su desempeño laboral..

Ello no obsta para que, según se pone de manifiesto en las actuaciones, las imágenes obtenidas, fueran aportadas por la empresa de seguridad, para la que presta

sus servicios el denunciante, para demostrar los hechos de los que se le acusaba en el ámbito laboral derivado del problema de seguridad creado.

De este modo, junto con la finalidad propia de las videocámaras instaladas, vinculadas a la seguridad, no puede desconocerse que, en determinados supuestos -como el que es objeto de las presentes actuaciones-, de la captación legítima de las imágenes por parte del responsable del fichero puedan derivar consecuencias de índole diversa, tanto en el ámbito penal, como administrativo, o incluso laboral, circunstancia que se produce con más habitualidad en el colectivo de vigilantes de seguridad por el trabajo desempeñado.

V

Se deben estudiar las implicaciones que lo denunciado presenta al respecto del derecho a la protección de datos en relación con el derecho a la tutela judicial efectiva de los protagonistas, por lo que partiremos de un análisis general relativo a la conexión de dichos derechos. Así, al respecto del derecho a la tutela judicial efectiva, nuestra norma suprema en el artículo 24 de la Constitución Española, en sus apartados 1 y 2, dispone lo siguiente:

“1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa.”

Así, constitucionalmente se consagra el derecho de los ciudadanos, ya sean personas físicas o jurídicas, a la tutela judicial efectiva y al derecho a utilizar los medios de prueba que consideren adecuados para el sostenimiento de su pretensión en sede judicial. Sin embargo, de dicha previsión, surge una colisión entre el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva de los jueces y tribunales referida, contenido en el artículo 24 de la Constitución, anteriormente transcrito, dadas a los bienes jurídicos afectados en su aplicación.

Por ello, ante tales situaciones, el Legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio Legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En efecto, la exigibilidad del consentimiento del titular de los datos que pudieran ser objeto de un tratamiento en un procedimiento judicial, para dicho tratamiento de sus datos, supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que una persona pueda ejercer, en plenitud, su derecho a la tutela

judicial efectiva. Así, la falta de estos datos o la dependencia en su aplicación a quien manejara la titularidad del dato, implicaría, 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.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) *“el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”*.

Por otro lado, junto a lo dispuesto en el artículo 6.2 de la LOPD, el artículo 11 de la LOPD, recoge otras excepciones, a la exigencia del consentimiento:

“1.- Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2.-El consentimiento exigido en el apartado anterior no será preciso:

a.-Cuando la cesión esté autorizada en una ley.(...)

d.-Cuando 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, en el ejercicio de las funciones que tiene atribuidas.(...)”(el subrayado es de la Agencia Española de Protección de Datos).

En este sentido, entraría en liza lo dispuesto en el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil, que admite la aportación como medio de prueba, de medios de reproducción de imágenes que sean relevantes para el proceso. Así establece, el precitado artículo:

“1. Los medios de prueba de que se podrá hacer uso en juicio son:

1. Interrogatorio de las partes.
2. Documentos públicos.
3. Documentos privados.
4. Dictamen de peritos.
5. Reconocimiento judicial.

6. Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso..

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”.

Por lo tanto, en cuanto a lo aportado en un juicio, dicho cuerpo legal admite la aportación como medio de prueba de los medios de reproducción de la palabra, el sonido y la imagen, lo cual implica la posibilidad de tratamiento de datos dentro de dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifestara sobre la legitimidad de lo presentado. Además, hemos de tener en cuenta que, la Audiencia Nacional en sentencia de 22 de octubre de 2010 (rec. 409/2009) nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

“De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002 . Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la

función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE, hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales."

Así las cosas, es el órgano judicial correspondiente quien se debe manifestar sobre la legitimidad de la prueba aportada, y en el caso que nos ocupa se ha manifestado sobre su legitimidad en la propia sentencia dictada, dado que fue admitida aunque de ella no se derivasen los elementos incriminatorios pretendidos por la empresa de seguridad.

VI

Por otro lado y a mayor abundamiento, la grabación objeto de denuncia data del 6 de julio de 2012 y la carta de sanción al denunciante de fecha 8 de agosto de 2012. Si el citado hecho fuera constitutivo de infracción (aun cuando como ya se ha desarrollado no da lugar) sería de carácter grave, según se recoge en el artículo 44.3.d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), *que señala: Son infracciones graves:... d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituyan infracción muy grave*".

Asimismo el artículo 47 de la LOPD señala:

"1. Las infracciones... graves prescribirán a los dos años...

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador..."

Respecto del cómputo de la prescripción el artículo 132.2 de la LRJPAC *"2. El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviera paralizado más de un mes por causa no imputable al presunto responsable."*

El computo de prescripción de la infracción comienza a contar en el día de la comisión de ésta y termina cuando se dicta el acuerdo de inicio con conocimiento del denunciado, es decir, el día que éste recibe la notificación.

La prescripción, responde al principio de seguridad jurídica, que garantiza que los administrados no queden, indefinidamente, sometidos al ejercicio por la administración de su poder sancionador, y puedan conocer con certeza, el momento en que no serán sancionados por el ilícito cometido. Así lo ha entendido la jurisprudencia al considerar que la prescripción opera con el fin de que sea pronta la reacción social al incumplimiento de la normativa protegida por la amenaza de la sanción prevista en la ley administrativa (STS de 13 de febrero de 1991).

En el presente caso, las grabaciones, objeto de denuncia, son de fecha 6 de julio de 2012 y la carta de sanción al denunciante aportando como prueba dichas imágenes es de fecha 8 de agosto de 2012; la denuncia por tales hechos se recibe en esta Agencia el 27 de noviembre de 2014, tras casi 16 meses desde los hechos denunciados.

El plazo de prescripción comienza a contarse el día que se cometió la presunta infracción, en el presente caso el “dies a quo” del cómputo prescriptivo debe fijarse en la fecha de la citada grabación. Por lo tanto, dado el tiempo transcurrido desde la supuesta actuación constitutiva de las posibles infracciones, hasta la fecha de presentación de la denuncia, se habría producido la prescripción de la presunta infracción que, en su caso se hubiera producido, a tenor del artículo 47 de la LOPD, que establece en dos años las infracciones graves.

Así la Sentencia de la Audiencia Nacional de 7 de junio de 2005 dice *“sólo podrá operar con efecto interruptor del plazo de prescripción la fecha de comunicación al interesado del acuerdo de iniciación del expediente sancionador...”*

Por su parte el artículo 122.4 del Reglamento de la LOPD establece que las actuaciones de investigación podrán durar hasta 12 meses.

VII

Seguidamente, procede analizar si el tratamiento de las imágenes realizado cumplía o no con los restantes requisitos exigibles en materia de protección de datos de carácter personal, recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de aquéllos de impresos en que se detalle la información; la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos.

A este respecto, el artículo 5.1 de la LOPD, que obliga a que se cumpla con el

deber de informar a los afectados, dispone que:

“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”.

En cuanto al modo en que debe facilitarse la información recogida en el artículo 5 de la LOPD, el artículo 3 de la Instrucción 1/2006, establece lo siguiente:

“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.”

“ANEXO-

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.”

En el caso que nos ocupa, según consta en el expediente, se aporta por CARREFOUR fotografías de la existencia de carteles informativos de zona videovigilada, ubicados en distintos puntos de acceso al establecimiento, informándose sobre la existencia de cámaras, y el responsable del sistema, de acuerdo al artículo 3. a) de la Instrucción 1/2006. Asimismo, se aporta modelo de cláusula informativa a disposición de los interesados de conformidad con el artículo 3. b) de la citada Instrucción.

En consecuencia, el sistema de captación de imágenes por medio de cámaras o videocámaras al que se refieren las presentes actuaciones cumple con el deber de información recogido en el artículo 5 de la LOPD.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.”

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se recoge en la Instrucción 1/2006, al señalar en su artículo 7 que:

“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.”

Pues bien, en el Registro General de Protección de Datos de la Agencia Española

de Protección de Datos, consta debidamente inscrito el fichero denominado VIDEOVIGILANCIA, cuyo responsable es **CARREFOUR NORTE, S.L.**

Asimismo, de acuerdo con dicha inscripción, los “Colectivos o categorías de interesados” a los que el fichero se refiere son: *“Clientes y usuarios, empleados, proveedores, personas que acceden a las sedes y establecimientos”*.

VIII

Por otro lado, en cuanto a la cesión a terceros denunciada, para analizar esta cuestión, debe partirse de los conceptos de responsable y encargado del tratamiento contenidos en la Ley Orgánica 15/1999.

Así, será responsable del fichero o del tratamiento, conforme al artículo 3 d) de la Ley, *“la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”*. Por su parte, es encargado del tratamiento, según el artículo 3 g), *“la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”*.

A este respecto el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), establece como regla general el previo consentimiento del interesado para la comunicación de datos personales a un tercero. Así dispone en su apartado 1 lo siguiente: *“1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.”*

El artículo 3. i) de la citada norma define la “cesión o comunicación de datos” como *“toda revelación de datos realizada a una persona distinta del interesado”*.

No obstante lo anterior, la propia LOPD habilita, en su artículo 12, el acceso de terceros a los datos personales cuando el acceso a los datos se realice para prestar un servicio al responsable del fichero o del tratamiento, al señalar en su apartado 1: *“1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.”*

El citado artículo 12.1 de la LOPD permite, por tanto, el acceso a datos de carácter personal a la persona o entidad que presta un servicio al responsable del fichero, sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión o comunicación de datos.

Pues bien, en el caso que se plantea el responsable de las instalaciones y el sistema de videovigilancia es la entidad **CARREFOUR, y SEGURIBER S.L.U.** era la entidad encargada de los servicios de seguridad privada del establecimiento, en virtud de contrato suscrito con fecha 1 de febrero de 2012, si bien dicho contrato fue resuelto en fecha 1 de septiembre de 2012. La finalidad de dicho contrato quedaba reflejada en la cláusula segunda del mismo en los siguientes términos: *“Que el objeto de este contrato es la prestación por parte de la empresa de un servicio de : vigilancia y*

protección, protección de personas...”

Así la citada empresa de seguridad actuaría por cuenta del responsable del fichero, en este caso **CARREFOUR**, no entendiéndose la existencia de una cesión de datos ilegítima, siendo el acceso a los datos por parte de **SEGURIBER S.L.U...**, necesarios para la prestación de un servicio al responsable del tratamiento.

Por lo tanto, no se considera que la utilización de las cámaras para la finalidad denunciada incumpla lo establecido en el artículo 12.4 de la LOPD que establece: *“En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”*.

A la vista de todo lo expuesto se procede al archivo del presente expediente, al no apreciarse vulneración a la normativa de protección de dato.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

- **PROCEDER AL ARCHIVO** de las presentes actuaciones.
- **NOTIFICAR** la presente Resolución a **CARREFOUR NORTE, S.L., SEGURIDAD PRIVADA SEGURIBER S.L.U.** y a D. **A.A.A..**

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