

- **Expediente N.º: EXP202204455**

## RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

### ANTECEDENTES

PRIMERO: **A.A.A.** (en adelante, la parte reclamante) con fecha 8 de abril de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **B.B.B.**, con NIF **\*\*\*NIF.1** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

1. Instalación de cámaras de seguridad, con aviso a los trabajadores a mediados de 2021, omitiendo que dichas cámaras graban audio y el lavabo del establecimiento, el cual no tiene puerta.

Indica que una de las cámaras, instalada en el año 2020, está situada encima del mostrador, enfocando hacia la entrada, y graba las conversaciones de los clientes y los trabajadores. La otra cámara, instalada en enero de 2021, se ubica detrás del panel del mostrador, enfocando el almacén y el acceso al baño (aporta imágenes sobre la ubicación de las cámaras).

Entiende que la grabación de sonido es desproporcionada y no justificada por la actividad desarrollada.

2. Los trabajadores no fueron informados sobre la utilización del sistema de videovigilancia para control laboral o sobre la finalidad de preservar la seguridad de las personas y bienes, ni tampoco que dicho sistema incorporase grabación de audio.

Además, el cartel de aviso no se encuentra fácilmente visible, ni para los trabajadores ni para el público, ya que está casi tapado por el aparato de aire acondicionado y situado en un lateral del establecimiento (no es posible verlo al entrar en el local por lo que no está ubicado en lugar visible para los clientes del establecimiento); no informa sobre el tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos reconocidos a los interesados; y hace referencia a la anterior normativa (aporta fotografía acreditativa de estas circunstancias).

3. Los trabajadores tienen acceso a las grabaciones realizadas por las cámaras de videovigilancia, dado que algunas son enviadas al teléfono móvil de la empresa, que se encuentra permanentemente en el establecimiento a disposición de todos los trabajadores, incumpliendo la normativa sobre conservación de las grabaciones.

La parte reclamante señala, asimismo, que el responsable envió enlaces a las grabaciones a través del grupo de whatsapp de la empresa, permitiendo a todos los

trabajadores acceder a las mismas.

Aporta un video acreditativo del envío a través de whatsapp de un enlace a una grabación procedente del sistema de videovigilancia objeto de la reclamación. La grabación en cuestión incluye sonido (se escuchan las voces de las personas captadas en dicha grabación, trabajadores y clientes).

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 20/04/2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 19/25/2022, en su respuesta al traslado de la reclamación, la parte reclamada informa lo siguiente:

. El sistema tiene dos cámaras que se encuentran en el interior del local y sólo graban el mismo. Se afirma que las imágenes se almacenan por espacio de 30 días en una cámara y de 3 horas en otra.

Aporta imágenes del campo de visión de las cámaras, en las que no se aprecia que capte el aseo indicado en la reclamación.

. Adjunta fotografías del cartel informativo expuesto en el establecimiento.

Se comprueba que se encuentra ubicado en el mismo lugar indicado en la reclamación, si bien su contenido ha sido modificado para que sea acorde con la normativa de protección de datos. Se comprueba que en lugar de informar sobre la identidad del responsable hace referencia al nombre comercial del establecimiento; informa sobre el ejercicio de derechos y cita una normativa no vigente.

. Se indica que las cámaras no graban sonido y para acreditarlo se aporta un pantallazo de la aplicación del móvil que gestiona el sistema en la que aparece la indicación manuscrita “desconectado” en la opción correspondiente al sonido, la cual puede volver a activar en cualquier momento de forma rápida y fácil, tan solo con desplazar la pestaña.

. Se aporta un escrito con la firma de la parte reclamante, para justificar que ha informado a los trabajadores de la política de uso de los dispositivos puestos a disposición de los trabajadores por el empleador, junto con otro escrito de confidencialidad que también firman los trabajadores, en el que se indica que el trabajador autoriza la visualización de su imagen en los circuitos internos de seguridad instalados por la empresa.

En ninguno de estos escritos se señala expresamente que una de las finalidades del sistema de vídeo vigilancia del establecimiento sea la del control laboral de los trabajadores.

. Por último, se manifiesta que al sistema sólo accede el propietario, responsable del tratamiento a través de su móvil con usuario y contraseña.

No aporta, en cambio, ninguna información en relación con el chat del trabajo y la remisión al mismo de vídeos grabados por el sistema de seguridad, como el que se aporta con la reclamación, a pesar de haber sido requerido para ello en la solicitud de información que le fue remitida.

TERCERO: Con fecha 16 de junio de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 05/08/2022, por la Subdirección General de Inspección de Datos se accede a la información relativa a la parte reclamada en “Axesor” (“Informe monitoriza”). (...).

QUINTO: Con fecha 10/08/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción de los artículos 13 y 6 del RGPD, tipificadas en los artículos 83.5.b) y 83.5.a) del mismo Reglamento, y calificadas como muy graves a efectos de prescripción en los artículos 72.1.h) y 72.1.b) de la LOPDGDD, respectivamente.

En el acuerdo de apertura se determinó que la sanción que pudiera corresponder, atendidas las evidencias existentes en el momento de la apertura y sin perjuicio de lo que resulte de la instrucción, ascendería a un total 3.000 euros (tres mil euros): 1.000 euros (mil euros) por la presunta infracción del artículo 13 del RGPD y de 2.000 euros (dos mil euros) por la presunta infracción del artículo 6 del RGPD.

Asimismo, se advertía que las infracciones imputadas, de confirmarse, podrán conllevar la imposición de medidas, según el citado artículo 58.2 d) del RGPD.

SEXTO: Con fecha 30/08/2022, tuvo entrada en esta Agencia escrito de la parte reclamante mediante el que comunica que desiste de la reclamación que ha dado lugar a las actuaciones.

SÉPTIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la LPACAP, se recibió escrito de alegaciones de la parte reclamada, en el que solicita el archivo del procedimiento. En relación con los hechos que han determinado la apertura del presente procedimiento sancionador, la parte reclamada formula las manifestaciones siguientes:

. El sistema de videovigilancia instalado cuenta con dos cámaras que no graban sonido.

. Con su escrito de respuesta al trámite de traslado acompañó fotografías de los carteles que avisan sobre la existencia de videovigilancia y la notificación

personalizada y con acuse de recibo que se hizo al respecto a los trabajadores.

Con sus alegaciones, la parte reclamada no aporta documento alguno, y solicita que se realice una inspección en el local para verificar la licitud del sistema.

OCTAVO: Con fecha 09/09/2022 se formuló propuesta de resolución en el sentido siguiente:

1. Que se sancione a la parte reclamada, por una infracción del artículo 13 del RGPD, tipificada en el artículo 83.5.b) del mismo Reglamento, y calificada como muy grave a efectos de prescripción en el artículo 72.1.h) de la LOPDGDD, con una multa de 1.000 euros (mil euros).
2. Que se sancione a la parte reclamada, por una infracción del artículo 6 del RGPD, tipificada en el Artículo 83.5.a) del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, con una multa de 2.000 euros (dos mil euros).
3. Que se imponga a la parte reclamada, en el plazo que se determine, la adopción de las medidas necesarias para adecuar su actuación a la normativa de protección de datos personales, con el alcance expresado en los Fundamentos de Derecho de la propuesta de resolución.

NOVENO: La propuesta de resolución reseñada en el Antecedente Octavo fue notificada a la parte reclamada. En dicha notificación se le concedía plazo para formular alegaciones frente a la propuesta de resolución, el cual transcurrió sin que en esta Agencia se haya recibido escrito alguno.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

### HECHOS PROBADOS

1. La parte reclamada es responsable del sistema de videovigilancia instalado en el establecimiento abierto al público en el que desarrolla su actividad económica.
2. En relación con el sistema de videovigilancia reseñado en el Hecho Probado Primero, la parte reclamada colocó un cartel informativo en un lateral del establecimiento, en su parte superior, parcialmente tapado por un aparato de aire acondicionado. Dicho cartel no informaba sobre el tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos reconocidos a los interesados; y hacía referencia a la anterior normativa (aporta fotografía acreditativa de estas circunstancias).

Dicho cartel fue sustituido por otro una vez conocida la reclamación por la parte reclamada. Este nuevo cartel, que se encuentra ubicado en el mismo lugar indicado en el párrafo anterior, en lugar de informar sobre la identidad del responsable hace

referencia al nombre comercial del establecimiento; informa sobre el ejercicio de derechos y cita una normativa no vigente.

3. Consta en las actuaciones un documento con el rótulo “Compromiso de confidencialidad de empleados”, dispuesto por la parte reclamada para que sean suscritos por sus empleados. En este documento, en relación con el sistema de videovigilancia instalada en el establecimiento, únicamente recoge la autorización del trabajador para la visualización de su imagen en los circuitos internos de seguridad instalados por la empresa.

4. El sistema de videovigilancia reseñado en el Hecho Probado Primero se gestiona a través de una aplicación instalada en el móvil de la parte reclamada. Esta aplicación permite activar o desactivar la opción correspondiente a la captación y grabación de sonido.

5. Consta incorporado a las actuaciones un video procedente del sistema de videovigilancia objeto de la reclamación que incluye sonido (se escuchan las voces de las personas captadas en dicha grabación, trabajadores y clientes).

## FUNDAMENTOS DE DERECHO

### I

#### Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *“Los procedimientos tramitados por la Agencia Española de Protección de Datos se registrarán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos”*.

### II

Con carácter previo debe señalarse que el artículo 63.1 de la LPACAP determina que *“los procedimientos de naturaleza sancionadora se iniciarán siempre de oficio por acuerdo del órgano competente”*, estableciéndose en el artículo 68 de la LOPDGDD que corresponde a la *“Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora”*. Así, que la parte reclamante desista de su reclamación resulta irrelevante y no implica el archivo o finalización del procedimiento sancionador incoado, toda vez que el mismo se inicia y se tramita en todas sus fases de oficio.

### III

#### La imagen y la voz son un dato personal

La imagen física y la voz de una persona, a tenor del artículo 4.1 del RGPD, son un dato personal y su protección, por tanto, es objeto de dicho Reglamento. En el artículo 4.2 del RGPD se define el concepto de "tratamiento" de datos personales.

Las imágenes y la voz captadas por un sistema de cámaras o videocámaras son datos de carácter personal, por lo que su tratamiento está sujeto a la normativa de protección de datos.

Es, por tanto, pertinente analizar si el tratamiento de datos personales (imagen y voz de la parte reclamante u de otras personas que presten servicio como empleadas en la empresa de la parte reclamada, y de las personas físicas que acuden como clientes al establecimiento de dicha empresa, abierto al público) llevado a cabo a través del sistema de videovigilancia denunciado es acorde con lo establecido en el RGPD.

### IV

#### Infracción

El artículo 12.1 del RGPD indica que quien lleve a cabo un tratamiento de datos personales, como es la captación de imágenes mediante un sistema de videovigilancia, deberá suministrar a los interesados la información indicada en los artículos 13 y 14 del RGPD.

Con la finalidad de que el deber de información previsto en el artículo 12 del RGPD se cumpla de manera concisa y comprensible para el afectado, el citado artículo 22 de la LOPDGDD prevé en relación con la videovigilancia un sistema de "información por capas".

En este sentido, la primera capa ha de referirse, al menos, a la existencia del tratamiento (videovigilancia), la identidad del responsable, la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD y dónde obtener más información sobre el tratamiento de los datos personales.

La información de la segunda capa debe estar disponible en un lugar fácilmente accesible al afectado, ya sea una hoja informativa en una recepción, cajero, etc..., colocada en un espacio público visible o en una dirección web, y ha de referirse al resto de elementos del artículo 13 del RGPD.

No es necesario especificar la ubicación precisa del equipo de videovigilancia.

Este deber de información se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible, y como mínimo, en los accesos a las zonas vigiladas ya sean interiores o exteriores. En caso de que el espacio videovigilado disponga de varios accesos deberá disponerse de dicho distintivo de zona videovigilada en cada uno de ellos.

Esta información debe suministrarse por adelantado -considerando 39 del RGPD-. El



objetivo es que quede claro el contexto de la vigilancia.

Por otra parte, el artículo 6.1 del RGPD establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

La implantación permanente de un sistema de cámaras de video por razones de seguridad tiene base legítima en la LOPDGDD, cuya exposición de motivos indica:

*“Junto a estos supuestos se recogen otros, tales como la videovigilancia... en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679”.*

En cuanto al tratamiento con fines de videovigilancia, el artículo 22 de la LOPDGDD establece que las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Este mismo artículo 22, en su apartado 8, dispone que *“El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica”.*

Sobre la legitimación para la implantación de sistemas de videovigilancia en el ámbito laboral, se tiene en cuenta el Real Decreto Legislativo 1/1995, de 24/03, que aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (LET), cuyo artículo 20.3 señala:

*“3. 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”.*

Entre las medidas de vigilancia y control admitidas se incluye la instalación de cámaras de seguridad, si bien estos sistemas deberán responder siempre al principio de proporcionalidad, es decir, el uso de las videocámaras debe ser proporcional al fin perseguido, esto es garantizar la seguridad y el cumplimiento de las obligaciones y deberes laborales.

El artículo 89 de la LOPDGDD, referido específicamente al *“derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo”* y al tratamiento de datos personales obtenidos con sistemas de cámaras o videocámaras para el ejercicio de funciones de control de los trabajadores, permite que los empleadores puedan tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

En relación con la grabación de sonidos, el citado artículo 89 de la LOPDGDD

establece lo siguiente:

*“2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.*

*3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley”.*

Por otra parte, interesa destacar que, según doctrina del Tribunal Constitucional, la grabación de conversaciones entre trabajadores o entre éstos y clientes no se justifica por la verificación del cumplimiento por el trabajador de sus obligaciones o deberes. En Sentencia de fecha 10/04/2000 (2000/98), dictada en el rec. núm. 4015/1996, se declara lo siguiente:

*“En este sentido debe tenerse en cuenta que el poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva y reconocido expresamente en el art. 20 LET, atribuye al empresario, entre otras facultades, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales (art. 20.3 LET). Mas esa facultad ha de producirse en todo caso, como es lógico, dentro del debido respeto a la dignidad del trabajador, como expresamente nos lo recuerda la normativa laboral (arts. 4.2.e y 20.3 LET)...*

*... debe recordarse que la jurisprudencia de este Tribunal ha insistido reiteradamente en la plena efectividad de los derechos fundamentales del trabajador en el marco de la relación laboral, ya que ésta no puede implicar en modo alguno la privación de tales derechos para quienes prestan servicio en las organizaciones productivas... En consecuencia, y como también ha afirmado este Tribunal, el ejercicio de tales derechos únicamente admite limitaciones o sacrificios en la medida en que se desenvuelve en el seno de una organización que refleja otros derechos reconocidos constitucionalmente en los arts. 38 y 33 CE y que impone, según los supuestos, la necesaria adaptabilidad para el ejercicio de todos ellos...*

*Debe por ello rechazarse la premisa de la que parte la Sentencia recurrida, consistente en afirmar que el centro de trabajo no constituye por definición un espacio en el que se ejerza el derecho a la intimidad por parte de los trabajadores, de tal manera que las conversaciones que mantengan los trabajadores entre sí y con los clientes en el desempeño de su actividad laboral no están amparadas por el art. 18.1 CE y no hay razón alguna para que la empresa no pueda conocer el contenido de aquéllas, ya que el referido derecho se ejercita en el ámbito de la esfera privada del trabajador, que en el centro de trabajo hay que entenderlo limitado a los lugares de descanso o esparcimiento, vestuarios, lavabos o análogos, pero no a aquéllos lugares en los que se desarrolla la actividad laboral...*

*...Tal afirmación resulta rechazable, pues no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores, como podría serlo la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que se aborden cuestiones ajenas a la relación laboral que se integran en lo que hemos denominado propia esfera de desenvolvimiento del individuo (SSTC 231/1988, de 2 de diciembre, FJ 4 y 197/1991, de 17 de octubre, FJ 3, por todas). En suma, habrá que atender no solo al lugar del centro del trabajo en que se instalan por la empresa sistemas audiovisuales de control, sino también a otros elementos de juicio (si*



*la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc.) para dilucidar en cada caso concreto si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores. Ciertamente, la instalación de tales medios en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta, a fortiori, lesiva en todo caso del derecho a la intimidad de los trabajadores, sin más consideraciones, por razones obvias... Pero ello no significa que esa lesión no pueda producirse en aquellos lugares donde se realiza la actividad laboral, si concurre alguna de las circunstancias expuestas que permita calificar la actuación empresarial como ilegítima intrusión en el derecho a la intimidad de los trabajadores. Habrá, pues, que atender a las circunstancias concurrentes en el supuesto concreto para determinar si existe o no vulneración del art. 18.1 CE.*

*...su limitación [de los derechos fundamentales del trabajador] por parte de las facultades empresariales sólo puede derivar bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho (SSTC 99/1994, FJ 7, y 106/1996, FJ 4), bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador (SSTC 99/1994, FJ 7, 6/1995, FJ 3 y 136/1996, FJ 7)...*

*Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que, si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes. Se trata, en definitiva, de la aplicación del principio de proporcionalidad...*

*La cuestión a resolver es, pues, si la instalación de micrófonos que permiten grabar las conversaciones de trabajadores y clientes en determinadas zonas... se ajusta en el supuesto que nos ocupa a las exigencias indispensables del respeto del derecho a la intimidad. Al respecto hemos de comenzar señalando que resulta indiscutible que la instalación de aparatos de captación y grabación del sonido en dos zonas concretas... no carece de utilidad para la organización empresarial, sobre todo si se tiene en cuenta que se trata de dos zonas en las que se producen transacciones económicas de cierta importancia. Ahora bien, la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar...*

*En resumen, la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes...). Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores..., comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores... mantengan entre sí o con los clientes”.*

## Obligaciones en materia de videovigilancia

De conformidad con lo expuesto, el tratamiento de imágenes a través de un sistema de videovigilancia, para ser conforme con la normativa vigente, debe cumplir los requisitos siguientes:

1.- La personas físicas o jurídicas, públicas o privadas, pueden establecer un sistema de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Se ha de valorar si la finalidad pretendida puede lograrse de otra forma menos intrusiva para los derechos y libertades de los ciudadanos. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios, considerando 39 del RGPD.

2.- Las imágenes obtenidas no puedan utilizarse para una finalidad ulterior incompatible con la que motivó la instalación del sistema de videovigilancia.

3.- Se deberá cumplir con el deber de informar a los afectados previsto en los artículos 12 y 13 del RGPD, y 22 de la LOPDGDD.

En tal sentido, el artículo 22 de la LOPDGDD prevé en relación con la videovigilancia un sistema de “información por capas”.

La primera capa ha de referirse, al menos, a la existencia del tratamiento (videovigilancia), la identidad del responsable, la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD y dónde obtener más información sobre el tratamiento de los datos personales.

Esta información se contendrá en un dispositivo colocado en un lugar suficientemente visible y debe suministrarse por adelantado.

La información de la segunda capa debe estar disponible en un lugar fácilmente accesible al afectado, ya sea una hoja informativa en una recepción, cajero, etc..., colocada en un espacio público visible o en una dirección web, y ha de referirse al resto de elementos del artículo 13 del RGPD.

4.- No pueden captarse imágenes de la vía pública, puesto que el tratamiento de imágenes en lugares públicos, salvo que concorra autorización gubernativa, sólo puede ser realizado por las Fuerzas y Cuerpos de Seguridad.

En algunas ocasiones, para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública.

Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o resulte imposible evitarlo por razón de la ubicación de aquéllas. Y, en tal caso extraordinario, las cámaras sólo podrán captar la porción mínima necesaria para preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Las cámaras instaladas no pueden obtener imágenes de espacio privativo de tercero y/o espacio público sin causa justificada debidamente acreditada, ni pueden afectar a la intimidad de transeúntes que transiten libremente por la zona.

No está permitida, por tanto, la colocación de cámaras hacia la propiedad privada de vecinos con la finalidad de intimidarlos o afectar a su ámbito privado sin causa justificada.

En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y en particular, no pudiendo afectar a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

No pueden captarse ni grabarse imágenes en espacios propiedad de terceros sin el consentimiento de sus titulares, o, en su caso, de las personas que en ellos se encuentren.

Resulta desproporcionado captar imágenes en espacios privados, tales como vestuarios, taquillas o zonas de descanso de trabajadores.

5.- Las imágenes podrán conservarse por un plazo máximo de un mes, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

En este segundo supuesto, deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

6.- El responsable deberá llevar un registro de actividades de los tratamientos efectuados bajo su responsabilidad en el que se incluya la información a la que hace referencia el artículo 30.1 del RGPD.

7.- El responsable deberá realizar un análisis de riesgos o, en su caso, una evaluación de impacto en la protección de datos, para detectar los derivados de la implantación del sistema de videovigilancia, valorarlos y, en su caso, adoptar las medidas de seguridad apropiadas.

8.- Cuando se produzca una brecha de seguridad que afecte a los tratamientos de cámaras con fines de seguridad, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo a la AEPD en un plazo máximo de 72 horas.

Se entiende por brecha de seguridad la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

9.- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que reúna los requisitos contemplados en el artículo 5 de la Ley 5/2014 de Seguridad Privada, de 4 de abril.

La Agencia Española de Protección de Datos ofrece a través de su página web [<https://www.aepd.es>] acceso a:

- . la legislación en materia de protección de datos personales, incluyendo el RGPD y la LOPDGDD (apartado “Informes y resoluciones” / “normativa”),
- . la Guía sobre el uso de videocámaras para seguridad y otras finalidades,
- . la Guía para el cumplimiento del deber de informar (ambas disponibles en el apartado “Guías y herramientas”).

También resulta de interés, en caso de realizar tratamientos de datos de bajo riesgo, la herramienta gratuita Facilita (en el apartado “Guías y herramientas”), que, mediante unas preguntas concretas, permite valorar la situación del responsable respecto del tratamiento de datos personales que lleva a cabo, y en su caso, generar diversos documentos, cláusulas informativas y contractuales, así como un anexo con medidas de seguridad orientativas consideradas mínimas.

## VI

### Infracción administrativa

No resulta controvertido en este caso el hecho de que la parte reclamada es la titular y responsable del sistema de videovigilancia denunciado y, por tanto, la responsable de los tratamientos de datos que conlleva la utilización de dicho sistema.

En relación con dicho sistema, se constata en este caso la existencia de un cartel informativo que no está ubicado en un lugar suficientemente visible ni incluye toda la información de primera capa que debe ofrecerse a los interesados, respecto de la identidad del responsable, la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD y dónde obtener más información sobre el tratamiento de los datos personales, además de citar una normativa no vigente.

Se considera que estos hechos vulneran lo establecido en el artículo 13 del RGPD, por lo que suponen la comisión de una infracción tipificada en el artículo 83.5 del RGPD, que dispone lo siguiente:

*“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

*(...)*

*b) los derechos de los interesados a tenor de los artículos 12 a 22; (...).”*

A efectos del plazo de prescripción de las infracciones, la infracción señalada en el párrafo anterior se considera muy grave conforme al artículo 72.1 de la LOPDGDD, que establece que:

*“En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

*(...)*

*h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta Ley Orgánica”.*

Además, la reclamación se basa en la presunta ilicitud del sistema de videovigilancia instalado por la parte reclamada en el local donde desarrolla su actividad empresarial, en relación con la grabación de sonidos, que ha sido debidamente acreditada por la parte reclamante con la aportación de un video captado por dicho sistema en el que constan grabadas las conversaciones de trabajadores y clientes que se encontraban en el establecimiento del responsable.

No consta en las actuaciones que el responsable haya informado a clientes y trabajadores sobre la captación de sus datos personales relativos a la voz de los interesados.

Tampoco la parte reclamada tiene en cuenta los límites previstos en el artículo 20.3 de la Ley del Estatuto de los Trabajadores (LET); lo establecido en el artículo 89.3 de la LOPDGDD, que admite la grabación de sonidos únicamente cuando resulten relevantes los riesgos y respetando los principios de proporcionalidad e intervención mínima; ni la doctrina del Tribunal Constitucional, ya expresada, según la cual la grabación de conversaciones entre trabajadores o entre éstos y clientes no se justifica por la verificación del cumplimiento por el trabajador de sus obligaciones o deberes.

En consecuencia, se entiende que la captación de la voz tanto de los trabajadores como de clientes de la parte reclamada para la función de videovigilancia pretendida no está motivada ni tiene amparo legal. Se tiene en cuenta que la grabación de voz supone una mayor intromisión en la intimidad.

Se considera que la parte reclamada realizó tratamientos de datos sin disponer de base legítima, vulnerando lo establecido en el artículo 6 del RGPD, lo que supone la comisión de una infracción tipificada en el artículo 83.5 del RGPD, que dispone lo siguiente:

*“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

*a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;”.*

A efectos del plazo de prescripción de las infracciones, la infracción señalada en el párrafo anterior se considera muy grave conforme al artículo 72.1.b) de la LOPDGDD, que establece que:

*“En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

*b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679”.*

En relación con los hechos constitutivos de estas infracciones, la parte reclamada, en su escrito de alegaciones a la apertura del procedimiento, se ha limitado a negar que el sistema capte sonidos, a pesar de las evidencias constatadas, como son la opción habilitada en la aplicación que gestiona dicho sistema, instalada en el dispositivo móvil de la parte reclamada, que permite activar o desactivar la captación y grabación de sonidos, así como el video aportado por la parte reclamante, en el que se escuchan las voces de trabajadores y clientes.

Lo mismo puede decirse respecto del incumplimiento del deber de informar. La parte reclamada reitera que dispone de un cartel informativo ubicado en el interior del establecimiento, pero no realiza manifestación alguna en relación con su inadecuada ubicación y con los defectos apreciados en la información que contiene.

En cuanto a la información ofrecida a los trabajadores, alega nuevamente que les notificó la existencia del sistema de videovigilancia, pero no acompaña ningún documento distinto al aportado con su respuesta al trámite de traslado de la reclamación, en el que no se informa a los trabajadores sobre la captación de sonidos. Según consta en el Hecho Probado Tercero, el documento al que se refiere la parte reclamada, que figura con el rótulo “Compromiso de confidencialidad de empleados”, en relación con el sistema de videovigilancia instalada en el establecimiento, únicamente recoge la autorización del trabajador para la visualización de su imagen en los circuitos internos de seguridad instalados por la empresa.

## VII Sanción

El artículo 58.2 del RGPD establece:

*“Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

*(...)*

*d) ordenar al responsable o encargado de tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;*

*(...)*

*i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular”.*

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en el artículo 58.2.d) del citado Reglamento es compatible con la sanción consistente en multa administrativa.

Con respecto a las infracciones de los artículos 13 y 6 del RGPD, se considera que la sanción que corresponde imponer es de multa administrativa.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD.

A fin de determinar la multa administrativa a imponer se han de observar las



previsiones del artículo 83.2 del RGPD, que señala lo siguiente:

*“2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*

- a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;*
- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*
- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción”.*

Por su parte, el artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD dispone:

*“1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.*

*2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:*

- a) El carácter continuado de la infracción.*
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.*
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.*
- f) La afectación a los derechos de los menores.*
- g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.*
- h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado”.*

El balance de las circunstancias contempladas, con respecto a las infracciones cometidas, permite fijar la valoración de la multa en 1.000 euros (mil euros) para la

infracción del artículo 13 del RGPD y de 2.000 euros (dos mil euros) para la infracción del artículo 6 del mismo Reglamento.

## VIII Medidas

Considerando las infracciones declaradas, procede imponer al responsable (la parte reclamada) la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *“ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado...”*.

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

No obstante, en este caso, con independencia de lo anterior, se acuerda requerir al responsable para que, en el plazo indicado en la parte dispositiva, acredite haber procedido a suprimir la captación de sonidos por el sistema de videovigilancia objeto de las actuaciones, así como el cumplimiento del deber de informar, facilitando a los trabajadores la información que exige el RGPD y completando la información que se ofrece mediante el cartel informativo instalado en el establecimiento, cuya ubicación deberá variarse para que sea fácilmente visible.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **B.B.B.**, con NIF **\*\*\*NIF.1**, por una infracción del artículo 13 del RGPD, tipificada en el Artículo 83.5.b) del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72.1.h) de la LOPDGDD, una multa de 1.000 euros (mil euros).

SEGUNDO: IMPONER a **B.B.B.**, con NIF **\*\*\*NIF.1**, por una infracción del artículo 6 del RGPD, tipificada en el Artículo 83.5.a) del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, una multa de 2.000

euros (dos mil euros).

TERCERO: REQUERIR a **B.B.B.** para que, en el plazo de un mes contado desde la notificación de la presente resolución, adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en el Fundamento de Derecho VIII de esta resolución, y justifique ante esta Agencia Española de Protección de Datos la atención del presente requerimiento.

CUARTO: NOTIFICAR la presente resolución a **B.B.B.**.

QUINTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la LPACAP, en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la

documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-120722

Mar España Martí  
Directora de la Agencia Española de Protección de Datos