



Expediente Nº: E/06676/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **QUALYTEL TELESERVICES, S.A.U.** en virtud de denuncia presentada ante la misma por Doña **A.A.A.** y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 11 de julio de 2014, tuvo entrada en esta Agencia escrito de Doña **A.A.A.** (en adelante la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **QUALYTEL TELESERVICES, S.A.U.** (en adelante el denunciado) instaladas en C/ Alcalá 265, Edif. 1 de Madrid.

La denunciante manifiesta que la citada empresa ha instalado tornos con toma de huellas, cámaras de videovigilancia en zonas de oficina: puestos de trabajo, entrada a aseos y zona de comedor, sin informar a los trabajadores ni al Comité de empresa.

Adjunta: reportaje fotográfico.

SEGUNDO: A la vista de los hechos denunciados, se realizaron por los Servicios de Inspección de esta Agencia actuaciones previas, con objeto de determinar si el tratamiento de los datos personales que se realiza, cumple con las condiciones que impone la citada normativa, teniendo conocimiento de las siguientes cuestiones:

Con fechas 14 de noviembre de 2014 y 4 de mayo de 2015, se solicitó información al responsable del establecimiento teniendo entrada en esta Agencia con fechas 1 de diciembre de 2014 y 19 de mayo de 2015 escritos en el que el representante de la de la sociedad del Grupo ARVATO BERTELSMANN denominada QUALYTEL TELESERVICES, S.A.U. (en adelante QUALYTEL), en calidad de Responsable del Departamento Jurídico del Grupo ARVATO BERTELSMANN manifiesta:

1. La mercantil QUALYTEL gestiona su sistema de videovigilancia a través de la empresa del Grupo que presta servicios corporativos: ARVATO IBERIA, S.L.U. Dicha empresa, presta los mismos servicios al resto de empresas del grupo empresarial ubicadas en el Edificio 1 del Centro de Negocios Alcalá 265.
2. El responsable del inmueble es la entidad IBERDROLA INMOBILIARIA, S.A.U. con domicilio social en el mismo Centro de Negocios Alcalá 265.
3. La empresa que realizó la instalación del sistema de videovigilancia fue la entidad PENTATEL COMUNICACIONES, S.L.

Se adjunta copia del presupuesto elaborado por dicha organización en fecha 07/10/2013 como Documento anexo nº1.

4. Respecto a las causas y la finalidad de la instalación, se determinó internamente la

necesidad de instalar videocámaras para garantizar la seguridad de las instalaciones, equipos y materiales, al amparo de la Ley de Seguridad Privada.

5. Respecto a la fotografía de los carteles informativos de zona videovigilada y su ubicación, en las fotos anexas, se reflejan los carteles informativos colocados en cada una de las plantas:
 1. Cámara nº 1 y cámara nº 4 de la Planta Baja del Edificio 1
 2. Cámara nº 5 de la Planta 1º del Edificio 1
 3. Cámara nº 8 de la Planta 2ª del Edificio 1
 4. Cámara nº 11 de la Planta 3ª del Edificio 1
 5. Cámara nº 15 de la Planta 4ª del Edificio 1

En el Edificio 1, todas las entradas: las de Planta Baja y las de ascensores de las diferentes Plantas del edificio, disponen del citado cartel informativo garantizando así que quien acceda vea siempre la información.

Los carteles informativos identifican la zona vigilada de modo que no se produzca el acceso de las personas sujetas a la videovigilancia sin la oportunidad de conocer la existencia de las videocámaras. En nuestro caso, los carteles informativos se encuentran situados en las puertas de entrada y no en las de emergencia (con la excepción de la puerta de entrada de emergencia de la Planta Baja) ni en cuartos CPD y SAU, para evitar identificar la ubicación concreta de cada cámara.

Se acompañan copia de los dos carteles informativos ubicados en el Edificio 1 como Documento anexo nº2. El motivo de establecer carteles informativos diferentes se justifica en la necesaria identificación de las entidades responsables de los ficheros de videovigilancia.

6. Con relación al modelo de formulario informativo a disposición de los interesados se anexa dicho formulario como Documento anexo nº3, indicando:
 1. Que en el Edificio 1 del Centro de Negocios de Alcalá 265 comparten instalaciones las siguientes entidades del Grupo ARVATO BERTELSMANN: QUALYTEL TELESERVICES, S.A.U.; TRÍA GLOBAL SERVICE, S.L.U.; QUALYTEL ANDALUCÍA, S.A.U.; ARVATO IBERIA, S.L.U.; ARVATO SERVICES AFTERSALES, S.A.U.; ARVATO SERVICES, SPAIN, S.A.U. Ya RVATO SERVICES IBERIA, S.A.U.
 2. Que el responsable del fichero es QUALYTEL TELESERVICES, S.A.U. (Planta Baja, Planta 1ª, Planta 2ª, Planta 3ª y Planta 4ª del Edificio 1); ARVATO IBERIA, S.L.U.; TRÍA GLOBAL SERVICE, S.L.U.; QUALYTEL ANDALUCÍA, S.A.U.; ARVATO SERVICES AFTERSALES, S.A.U.; ARVATO SERVICES, SPAIN, S.A.U. y ARVATO SERVICES IBERIA, S.A. U. (Planta Baja, Planta 3ª y Planta 4ª del Edificio 1).

El procedimiento establecido para distribuir los formularios ante una petición del mismo es dirigirse al mostrador de recepción del edificio, situado en la entrada principal de la Planta Baja y solicitar al personal de recepción una copia del mismo. Este personal, ante dicha demanda imprime el citado documento y se lo entrega al interesado en el momento.

7. El sistema de videovigilancia de las instalaciones del Edificio 1 dispone de 17

cámaras.

1. Las cámaras de la Planta Baja del Edificio 1 son las siguientes:
 - i. Cámara de puerta de entrada (nº 1 en el plano de Planta Baja)
 - ii. Cámara cuarto SAU (nº 2 en el plano de Planta Baja)
 - iii. Cámara puerta emergencia trasera (nº 3 en el plano de Planta Baja)
 - iv. Cámara puerta emergencia entrada (nº 4 en el plano de Planta Baja)
2. Las cámaras de la Planta 1ª del Edificio 1 son las siguientes:
 - i. Cámara ascensores (nº 5 en el plano de Planta 1ª)
 - ii. Cámara puerta emergencia izquierda (nº 6 en el plano de Planta 1ª)
 - iii. Cámara puerta emergencia derecha (nº 7 en el plano de Planta 1ª)
3. Las cámaras de la Planta 2ª del Edificio 1 son las siguientes:
 - i. Cámara ascensores (nº 8 en el plano de Planta 2ª)
 - ii. Cámara puerta emergencia izquierda (nº 9 en el plano de Planta 2ª)
 - iii. Cámara puerta emergencia derecha (nº 10 en el plano de Planta 2ª)
4. Las cámaras de la Planta 3ª del Edificio 1 son las siguientes:
 - i. Cámara ascensores (nº 11 en el plano de Planta 3ª)
 - ii. Cámara CPD (nº 12 en el plano de Planta 3ª)
 - iii. Cámara puerta emergencia izquierda (nº 13 en el plano de Planta 3ª)
 - iv. Cámara puerta emergencia derecha (nº 14 en el plano de Planta 3ª)
5. Las cámaras de la Planta 4ª del Edificio 1 son las siguientes:
 - i. Cámara ascensores (nº 15 en el plano de Planta 4ª)
 - ii. Cámara puerta emergencia izquierda (nº 16 en el plano de Planta 4ª)
 - iii. Cámara puerta emergencia derecha (nº 17 en el plano de Planta 4ª)

Todas las cámaras son fijas, no pueden hacer zoom ni disponen de motor o piezas móviles para su desplazamiento. Todas ellas están orientadas a las puertas de acceso a ascensores de cada Planta y a las puertas de emergencia, salvo 2 cámaras que están en el interior de los dos cuartos técnicos (SAU y CPD) en los que por defecto no debe acceder nadie salvo personal técnico o de mantenimiento.

En los 5 planos anexos se muestra la ubicación de las 17 cámaras instaladas:

- a. Plano Planta Baja: 4 cámaras. (Documento anexo nº 4)
- b. Plano Planta 1ª: 3 cámaras. (Documento anexo nº 5)
- c. Plano Planta 2ª: 3 cámaras. (Documento anexo nº 6)
- d. Plano Planta 3ª: 4 cámaras. (Documento anexo nº 7)
- e. Plano Planta 4ª: 3 cámaras. (Documento anexo nº 8)

Se observa en el plano de la Planta Baja que la cámara 3 está en dentro de la zona calificada como Comedor, aunque se encuentra direccionada hacia la puerta de emergencia trasera.

8. Se adjuntan las fotografías de cada cámara identificada en los planos y fotografía de la imagen captada por cada cámara identificada en los planos como Documento anexo nº 9.

Las fotografías muestran imágenes del interior del edificio, hacia puerta de entrada

al edificio, cuarto SAU, puertas de emergencia de entrada y trasera de planta baja, acceso a zona de ascensores en cada planta, puertas de emergencia de derecha e izquierda de plantas 1ª a 4ª y cuarto CPD.

Se observa que la imagen captada por la cámara nº 3 de la Planta Baja situada en la zona calificada como Comedor capta tablón de anuncios a la derecha, y a la izquierda puerta de emergencia y enfoca muy parcialmente una de las mesas del comedor.

9. No hay monitores dedicados a la visualización de las cámaras en ningún punto de la instalación ni fuera de ella. La conexión al servidor de las cámaras y las grabaciones se hace desde la red de sistemas por escritorio remoto.

El sistema de videovigilancia está alojado en un servidor físico en el mismo edificio, controlado por software.

10. Todas las cámaras son IP; conectadas a un switch de datos, conectado al servidor de grabación y visualización de las cámaras. El servidor de cámaras se encuentra en la sala técnica (CPD) de la tercera planta. A este servidor sólo puede accederse por escritorio remoto de forma lógica, o entrando en el CPD de forma física.
11. Las cámaras graban imágenes en modalidad 24x7. Las grabaciones se borran automáticamente al pasar 8 días de su creación, salvo en el supuesto de incidente en seguridad que son conservadas y únicamente pueden acceder a las grabaciones los siguientes cargos del Departamento IT: Responsable de servidores, Responsable de Redes, IT Manager Madrid y Director IT.
12. El fichero "VIDEOVIGILANCIA" de QUALYTEL fue inscrito en el Registro General de Protección de Datos (RGPD) de esa Agencia, en fecha 25/06/2008, con código de inscripción nº ***CÓD.1. No obstante, el pasado día 14/11/2014 se procedió a notificar a la AEPD la modificación de dicho asiento registral (nº de envío generado por el sistema NOTA: ***** en fecha 13/11/2014) informando al órgano de control del cambio de domicilio del responsable del fichero y del nuevo encargado del tratamiento.
13. Se adjunta copia del Documento de Seguridad de QUALYTEL como Documento anexo nº 10.

El apartado 10.5 contiene la Circular informativa sobre Protección de Datos de Carácter Personal.

14. El sistema de videovigilancia no se encuentra conectado con centrales receptoras de alarmas.
15. En las instalaciones de C/ Alcalá 265 existe un control de acceso mediante huella digital para los empleados.

Con la finalidad de identificar en el RGPD este novedoso control de accesos, el pasado día 14/11/2014 se procedió a notificar a la AEPD la modificación del fichero "PERSONAL" de QUALYTEL con código de inscripción nº ***CÓD.2 (nº de envío generado por el sistema NOTA: *****1 en fecha 13/11/2014) informando al órgano de control del cambio de domicilio del responsable del fichero, del nuevo encargado del tratamiento y de la inclusión del dato de la huella digital del colectivo

de trabajadores.

Mediante una diligencia se ha comprobado la inscripción de este fichero y del de VIDEOVIGILANCIA que constan modificados en fecha 20/11/2014.

16. Respecto al procedimiento utilizado para informar a los trabajadores de la finalidad del tratamiento del dato de la huella digital, manifiesta:

1. *Que QUALYTEL en el momento de implementar en la organización la medida de control de acceso a través de huella digital, tomó en consideración la doctrina de esa Agencia y la jurisprudencia al respecto, ya que esta parte comparte que la huella digital es un dato de carácter personal, tal y como se define en el artículo 3a) LOPD al permitir la identificación de una persona si dicho dato se vincula a su identidad, pese a que el tratamiento del dato biométrico no revela nuevas características referentes a su comportamiento.*

El sistema de control de acceso implantado por QUALYTEL es acorde con el principio de proporcionalidad ya que sólo recaba un parámetro físico para la identificación unívoca del empleado con la exclusiva finalidad del control de obligaciones derivadas de la relación laboral que vinculan al trabajador con la empresa.

Respecto a la necesidad de obtener el consentimiento informar que si bien el artículo 6.1 LOPD exige el consentimiento del interesado para el tratamiento de los datos de carácter personal, el artículo 6.2 de la citada normativa prevé que no será preciso el consentimiento cuando los datos “se refieran a las partes de una relación laboral y sean necesarios para su mantenimiento o cumplimiento”.

Por tanto, habiendo decidido la dirección de la empresa (en virtud del artículo 20.3 ET) implementar el sistema de control de accesos a las instalaciones mediante la huella digital del empleado, no se requiere el consentimiento del trabajador, quien solo requiere ser informado, atendiendo al artículo 5 LOPD.

2. *A raíz del cambio de domicilio social de la empresa y la posterior implantación del sistema de control de acceso QUALYTEL ha informado a su colectivo de trabajadores tal y como establece el artículo 5 LOPD.*

En este sentido, el procedimiento utilizado por QUALYTEL para informar al personal es el siguiente:

a) Respecto a los trabajadores en plantilla, la información necesaria ha sido facilitada a través de comunicado específico en el portal del empleado en la intranet corporativa que se gestiona mediante la herramienta facilitada por nuestro colaborador META 4.

Se adjunta copia del comunicado publicado por el Departamento de RR.HH en la Intranet corporativa accesible por los trabajadores en plantilla de QUALYTEL.

Este comunicado incluye la información relativa a la recogida de la huella digital finalidad así como la finalidad del fichero de videovigilancia.

Se adjunta como documentación acreditativa del cumplimiento del derecho de información para los actuales empleados en plantilla de QUALYTEL, copia del comunicado publicado en el portal del empleado (Documento anexo nº1)

b) Con relación al colectivo de nuevos trabajadores de QUALYTEL, a información LOPD consta en las correspondientes cláusulas adicionales anexas al contrato laboral que se suscriben al entrar a trabajar en cualquiera de las empresas que integran el Grupo ARVATO BERTELSMANN:

Se adjunta cláusula adicional séptima al contrato laboral, relativa a protección de datos de carácter personal, cuyo contenido es muy similar al reflejado en el comunicado informativo LOPD del portal del empleado corporativo.

Se adjunta como documentación acreditativa del cumplimiento del derecho de información para los nuevos empleados de QUALYTEL, copia de las cláusulas adicionales al contrato de trabajo (Documento anexo nº2).

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

En primer lugar procede situar el contexto normativo en materia de videovigilancia. 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.”

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.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

III

En el presente expediente se denuncia por parte de Doña **A.A.A.**, la existencia de un sistema de videovigilancia las oficinas de la entidad **QUALYTEL TELESERVICES, S.A.U.** ubicadas en C/ Alcalá 265, Edif. 1 de Madrid, donde la denunciante presta sus servicios, manifestando que la citada empresa ha instalado tornos con toma de huellas, cámaras de videovigilancia en zonas de oficina: puestos de trabajo, entrada a aseos y zona de comedor, sin informar a los trabajadores ni al Comité de empresa.

Ahora bien, en esta cuestión, en primer lugar se plantea si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD.

A este respecto es necesario realizar varias aclaraciones respecto al consentimiento en el ámbito laboral. Así, el consentimiento, elemento base en el tratamiento de los datos, entraña cierta complejidad, especialmente cuando nos referimos al ámbito laboral, dado que resulta de difícil cumplimiento que en ese ámbito concurren los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *“Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen”*.

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones

emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

La concurrencia de estos requisitos resulta de difícil cumplimiento en el ámbito laboral. En consecuencia, vista la dificultad que entraña obtener el consentimiento, la Agencia Española de Protección de Datos, ha entendido que lo procedente es acudir a las normas que legitimen el tratamiento de los datos. Por tanto, en el ámbito laboral, el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en ése articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”*.

De todo ello se desprende que el empresario, en este caso la entidad denunciada, se haya legitimada para tratar las imágenes de los trabajadores en el ámbito laboral, al amparo del artículo 20.3 del ET. Ahora bien, esta legitimación no es absoluta y exige por parte del empresario la obligación de informar de dicho tratamiento a los trabajadores (cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.).

Es necesario en este punto diferenciar si la instalación de la cámara en el centro de trabajo es como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales o si es una medida de seguridad para proteger la instalación y sus empleados.

En el presente caso y respecto al sistema de videovigilancia, la entidad denunciada ha manifestado que ha sido instalado para garantizar la seguridad de las instalaciones, equipos y materiales, al amparo de la Ley de Seguridad Privada. En este sentido, todas

las cámaras son fijas, no disponen de zoom ni de posibilidad de desplazamiento. Todas ellas están orientadas a las puertas de acceso a ascensores de cada Planta y a las puertas de emergencia, salvo 2 cámaras que están en el interior de los dos cuartos técnicos (SAU y CPD) en los que por defecto no debe acceder nadie salvo personal técnico o de mantenimiento.

Por otra parte, y respecto a los hechos denunciados relativos al sistema de control de personal, consta acreditado que en las instalaciones de C/ Alcalá 265 existe un control de acceso mediante huella digital para los empleados.

Asimismo, se significa que esta Agencia ha analizado en diversas ocasiones la naturaleza y la procedencia o improcedencia del tratamiento de la huella digital de los afectados en el citado contexto de control horario y jornada laboral.

Cabe entender por datos biométricos “aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos en un sujeto y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc.”.

Centrándonos en los datos de carácter personal que pueden ser considerados como “estáticos”, es decir, invariables a lo largo de la vida de la persona y ateniéndonos a la definición de dato de carácter personal contenida en el artículo 3.a) de la Ley Orgánica 15/1999 (LOPD), debe indicarse que si bien el procesamiento de estos datos biométricos no revela nuevas características referentes al comportamiento de las personas sí permite, lógicamente, su identificación, dado que, como se analiza en el documento del Grupo del artículo 29, en un gran número de supuestos su finalidad es precisamente la identificación del sujeto o el control de acceso a una determinada instalación o puesto de trabajo. Por ello, resulta evidente que, en caso de procederse a su tratamiento dicho tratamiento deberá ajustarse a la LOPD.

La evolución de la tecnología ha demostrado la utilidad del tratamiento de datos biométricos y, en particular, de la huella dactilar en el desarrollo de sistemas de identificación única de la población.

Dicho esto, y entrando en el análisis del tratamiento del dato de la huella dactilar del afectado, será preciso tomar en consideración como elementos esenciales para juzgar la conformidad de dicho tratamiento con las previsiones de la LOPD los principios de legitimación para el tratamiento de los datos y finalidad, en las distintas previsiones que en relación con éste último establece el artículo 4 de la LOPD.

Así, como también será necesario que el tratamiento se encuentre habilitado por alguna de las causas que en el derecho español autorizan el mismo. En particular, el artículo 6.1 de la LOPD dispone que “*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa*”. Fuera de estos casos, dispone el artículo 6.2 que “*no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación 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”.

Ello implicará que el tratamiento deberá encontrarse habilitado en una norma con rango de Ley, en el sentido amplio que se ha venido manteniendo por esta Agencia Española de Protección de Datos, o que el mismo sea necesario para el adecuado mantenimiento de una relación jurídica, en los términos previstos en el artículo 6.2 de la LOPD.

En la mayor parte de los supuestos, podrá aducirse la necesidad del tratamiento para el mantenimiento de una relación jurídica entre quien trata el dato y el afectado. De este modo, se viene a considerar por el responsable que la preexistencia de un vínculo jurídico, contractual o de otra índole, con el afectado posibilita el tratamiento de la huella dactilar, a fin de poder procederse al efectivo control del cumplimiento por el afectado de las obligaciones derivadas de esa relación jurídica.

Ello conduce al necesario análisis de los distintos principios vinculados con la finalidad que justifica el tratamiento y que, en particular, debe materializarse en los principios de proporcionalidad y prohibición del tratamiento con fines incompatibles a los que justificaron la recogida y tratamiento de los datos, consagrados en los artículos 4.1 y 4.2 de la LOPD.

Siguiendo la doctrina emanada por el Tribunal Constitucional, el cumplimiento del principio de proporcionalidad exigirá superar los principios de idoneidad, necesidad y proporcionalidad. Así, señala la Sentencia del Tribunal Constitucional 207/1996 que se trata de *“una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad”*, añadiendo que *“en este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)»”*

No existiendo duda alguna de que el tratamiento de los datos biométricos resulta idóneo para alcanzar las finalidades de control perseguidas, el problema estribará, precisamente en si en el supuesto planteado será posible alcanzar la finalidad perseguida a través de medios menos intrusivos en la esfera íntima del afectado con similar eficacia y si el uso de esta medida depara un mayor beneficio al interés general

que el perjuicio que eventualmente pueda ocasionarse al afectado. Ello irá vinculado al grado de necesidad de realización del tratamiento para el mantenimiento de la relación jurídica en que pretende justificarse el mismo con arreglo al artículo 6.2 de la LOPD.

Pues bien, la solución que haya de darse al juicio de proporcionalidad y necesidad, necesario para considerar que el tratamiento respeta lo dispuesto en el artículo 4.1 de la LOPD y se encuentra legitimado por el artículo 6.2 de la misma, no podrá ser única, debiendo en cada caso atender a la concreta finalidad perseguida, esto es, a la relación jurídica subyacente al tratamiento, a la situación del afectado y a las consecuencias que pudieran derivarse de la adopción de una medida menos gravosa para la intimidad del interesado.

En resumidas cuentas, deberán eludirse en el análisis juicios genéricos que conduzcan a respuestas únicas que no atiendan a las circunstancias del caso, a partir, al menos, de los tres parámetros que acaban de indicarse.

Tampoco sería adecuado considerar que el tratamiento de ese dato debería considerarse contrario a los principios de protección de datos cuando se lleva a cabo con una finalidad de control de acceso, dado que existirán supuestos en los que la garantía de la seguridad necesaria para el acceso a dichas instalaciones justifique el uso de este tipo de datos.

Tomando en cuenta este hecho, la Agencia Española de Protección de Datos ha atendido las distintas consultas que le han sido planteadas sobre esta cuestión, considerando la procedencia o improcedencia del tratamiento de la huella dactilar en virtud de las circunstancias de cada caso concreto.

Así, en reiteradas ocasiones, se ha considerado conforme a la LOPD el tratamiento del citado dato para controlar el cumplimiento por los trabajadores o empleados públicos de su jornada laboral, a tenor de las circunstancias concurrentes en esta categoría de afectados y la dificultad de establecer otros procedimientos igual de eficientes e idóneos para garantizar el efectivo cumplimiento de las obligaciones derivadas del contrato de trabajo o de la relación estatutaria que vincula al funcionario con la Administración Pública. Así, en informe de 28 de febrero de 2006 se señalaba lo siguiente:

“En efecto, en el ámbito de la relación jurídica que existe entre los trabajadores y el empresario al que prestan sus servicios, debe entenderse adecuado que éste recabe los datos que sean precisos para el normal desenvolvimiento de la misma y, dentro de estos datos, parece adecuado que se recaben del trabajador los necesarios para su identificación, a efectos de garantizar las medidas de seguridad que se consideren oportunas por parte de la empresa para que por la misma se pueda comprobar el grado de cumplimiento de las obligaciones que competen a los trabajadores.

Ello no obstante, deberá darse cumplimiento a lo dispuesto en el artículo 5 de la LOPD, dado que si bien no será preciso el consentimiento del interesado, si deberá advertirse al mismo de los extremos contenidos en ese precepto y, especialmente, de las consecuencias disciplinarias que podría acarrear su negativa a que la huella sea tratada.

Al propio tiempo, debe recordarse que los datos a los que se viene haciendo referencia podrían ser utilizados por el empresario única y exclusivamente para la función de control de la presencia del trabajador, tal y como se ha venido señalando, pero no para ninguna otra finalidad distinta, puesto que el artículo 4.2 de la Ley Orgánica 15/1999 dispone claramente que “Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”.

Por otra parte, no debe dejar de tenerse en cuenta la exigencia del artículo 4.2 de la LOPD que, en el sentido derivado de la Sentencias del Tribunal Constitucional 292/2000, de 30 de noviembre, impide el tratamiento de los datos para fines distintos de los que justificaron la recogida de los mismos. De este modo, la eventual proporcionalidad que pudiera encontrarse en el supuesto concreto quedaría completamente desvirtuada en caso de que los datos fueran empleados por el responsable para cualquier otra finalidad distinta de aquella respecto de la que se considera posible el tratamiento.

También, la conformidad a lo dispuesto en la LOPD del tratamiento de la huella digital para el control de cumplimiento de la jornada laboral ha sido indirectamente considerada por la Audiencia Nacional en sentencia de 4 de marzo de 2010, dictada en el recurso 234/2008, considerando que en este caso no sería preciso contar con el consentimiento de los trabajadores, sin perjuicio del ineludible cumplimiento por parte del empresario del deber de información establecido en el artículo 5 de la LOPD.

En el presente caso, se debe señalar que son partes afectadas de un lado, la entidad denunciada y, de otro, sus empleados, concurriendo entre ambos una relación jurídica de índole laboral que habilita a la empresa para el tratamiento de los datos personales de los trabajadores para las “finalidades” que tiene encomendadas, como es el caso del control horario, sin el consentimiento de los afectados, con base en lo dispuesto en el artículo 6.2 de la LOPD que recoge:

“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 comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento..”

Respecto al consentimiento en el ámbito laboral, el artículo 20.3 del Estatuto de los Trabajadores dispone que:

“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”

Por tanto, el tratamiento del dato personal de la huella dactilar para el “control de horario” obliga al responsable del tratamiento a cumplir con el deber de información a los afectados de forma previa y de buena fe.

Habida cuenta la denuncia formulada en contraposición con la normativa transcrita, la documentación aportada lleva a determinar que la entidad denunciada está informando a sus empleados sobre la implantación de un nuevo sistema de control a través de la lectura biométrica de la huella dactilar que cumple con el derecho de “información” citado y previo al tratamiento de los datos de los afectados.

En el presente supuesto, respecto al procedimiento utilizado para informar a los trabajadores de la finalidad del tratamiento del dato de la huella digital, la entidad denunciada ha acreditado que ha facilitado a su personal en plantilla la información necesaria a través de un comunicado específico en el portal del empleado en la intranet corporativa que se gestiona mediante la herramienta facilitada por META 4. QUALYTEL ha aportado copia del comunicado publicado por el Departamento de RR.HH en la Intranet corporativa accesible por los trabajadores en plantilla de QUALYTEL. Este comunicado incluye la información relativa a la recogida de la huella digital finalidad así como la finalidad del fichero de videovigilancia.

También ha remitido documentación acreditativa del cumplimiento del derecho de información para los actuales empleados en plantilla de QUALYTEL, enviando copia del comunicado publicado en el portal del empleado.

Por último, y con relación al colectivo de nuevos trabajadores de QUALYTEL, la información LOPD consta en las correspondientes cláusulas adicionales anexas al contrato laboral que se suscriben al entrar a trabajar en cualquiera de las empresas que integran el Grupo ARVATO BERTELSMANN: Se adjunta cláusula adicional séptima al contrato laboral, relativa a protección de datos de carácter personal, cuyo contenido es muy similar al reflejado en el comunicado informativo LOPD del portal del empleado corporativo y se adjunta como documentación acreditativa del cumplimiento del derecho de información para los nuevos empleados de QUALYTEL, copia de las cláusulas adicionales al contrato de trabajo.

En definitiva, cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, se aplicaría toda la normativa y jurisprudencia recogida “ut supra”, es decir sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD, disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

Sin embargo, en el caso que nos ocupa, el representante de la entidad denunciada ha manifestado que la finalidad del sistema de videovigilancia es la seguridad, sin que se aporten pruebas por parte de la denunciante que desvirtúen esta afirmación.

Así, el tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD el cual reza lo siguiente:

“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 hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que 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, la entidad denunciada, ha acreditado que cumple con el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, informando tanto a los visitantes de la entidad como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado, sin que conste su utilización a efectos de control laboral ni se informe, en consecuencia, del uso de sus imágenes a tal fin.

Por otra parte, ha acreditado que ha informado debidamente a sus trabajadores de

la finalidad del tratamiento del dato de la huella digital, la entidad denunciada ha acreditado que ha facilitado a su personal en plantilla la información necesaria a través de un comunicado específico en el portal del empleado en la intranet corporativa que se gestiona mediante la herramienta facilitada por META 4. QUALYTEL ha aportado copia del comunicado publicado por el Departamento de RR.HH en la Intranet corporativa accesible por los trabajadores en plantilla de QUALYTEL. Este comunicado incluye la información relativa a la recogida de la huella digital finalidad así como la finalidad del fichero de videovigilancia.

También ha remitido documentación acreditativa del cumplimiento del derecho de información para los actuales empleados en plantilla de QUALYTEL, copia del comunicado publicado en el portal del empleado.

Por último, y con relación al colectivo de nuevos trabajadores de QUALYTEL, la información LOPD consta en las correspondientes cláusulas adicionales anexas al contrato laboral que se suscriben al entrar a trabajar en cualquiera de las empresas que integran el Grupo ARVATO BERTELSMANN. Se adjunta cláusula adicional séptima al contrato laboral, relativa a protección de datos de carácter personal, cuyo contenido es muy similar al reflejado en el comunicado informativo LOPD del portal del empleado corporativo y se adjunta como documentación acreditativa del cumplimiento del derecho de información para los nuevos empleados de QUALYTEL, copia de las cláusulas adicionales al contrato de trabajo.

Por lo tanto, a la vista de todo lo expuesto, en el presente caso no se aprecia vulneración de la normativa de protección de datos por parte de la entidad denunciada por lo que procede el archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **QUALYTEL TELESERVICIOS, S.A.U.** y a Doña **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