

- **Expediente N.º: EXP202314832**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 13 de septiembre de 2023, se presentó reclamación con número de registro de entrada REGAGE23e00061290937 ante la Agencia Española de Protección de Datos contra VILLA DE PINTO, S.L. con NIF B87253043. Los motivos en que basa la reclamación son los siguientes:

La parte reclamante, trabajador en el establecimiento de la parte reclamada, manifiesta que el mismo dispone de un sistema de videovigilancia que capta imagen y sonido, habiéndose utilizado las captaciones de este para la sanción disciplinaria del reclamante y el despido de otro trabajador de la entidad.

Manifiesta que solicitó la supresión de las cámaras a la entidad, sin obtener resultado satisfactorio.

Aporta fotografía de una cámara, copia de la sanción disciplinaria al reclamante, copia del documento de despido disciplinario a otro trabajador de la entidad en el que se transcribe un fragmento de la conversación mantenida entre este trabajador y un cliente, solicitud de supresión de las cámaras y párrafos de contestación de la empresa.

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 VILLA DE PINTO, S.L 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 24/10/2023 como consta en el acuse de recibo que obra en el expediente.

Con fecha 16/11/2023 se recibe en esta Agencia escrito de respuesta indicando:

- El hotel cuenta con 12 cámaras de circuito interno y 6 cámaras con conexión remota: recepción y entrada del hotel, despacho, puerta y rampa de garaje, almacén, pasillos de las plantas, cocina, office, barra y sala y lavandería. Envía fotos de la situación de estas cámaras y de la señalización de las zonas videovigiladas.

- El circuito cerrado de videovigilancia del hotel solo es visible por el personal de recepción y dirección del hotel, no quedando expuesto al público en general ni personal no autorizado. Para el acceso a las grabaciones, únicamente se puede acceder mediante contraseña de la cual está en posesión el responsable designado y la Dirección. En cuanto a las cámaras remotas, solo disponen de acceso el responsable y la Dirección.
- Al iniciar la relación laboral, en el contrato de trabajo, en su cláusula cuarta, se informa al trabajador de la existencia de cámaras de seguridad.
- El circuito de circuito cerrado de televisión carece de sonido y la opción de sonido en las cámaras de acceso remoto está deshabilitada desde su instalación.
- En cuanto a la motivación de por qué se han utilizado las grabaciones del sistema de vídeo vigilancia de la empresa para sancionar disciplinariamente a un trabajador y para el despido disciplinario de otra trabajadora se basa en el art. 20.3 del Estatuto de los Trabajadores, en la jurisdicción europea y la jurisdicción ordinaria.

Las grabaciones se utilizaron para comprobar la veracidad de las quejas de otros trabajadores y clientes.

TERCERO: Con fecha 13 de diciembre de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

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

Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que VILLA DE PINTO, S.L realiza, entre otros tratamientos, la recogida y utilización de la imagen de aquellas personas que se encuentren dentro de su recinto, incluidos sus trabajadores, por medio de cámaras de videovigilancia.

VILLA DE PINTO, S.L ALIAS realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del citado artículo 4.7 del RGPD:

«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

III

Obligaciones en materia de videovigilancia

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.- El tratamiento de las imágenes mediante la instalación de sistemas de cámaras o videocámaras deberá ser lícito y ajustarse al principio de proporcionalidad y al de minimización de datos, en los términos ya señalados.

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 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.

En este caso, la parte reclamante, manifiesta que el mismo dispone de un sistema de videovigilancia que capta imagen y sonido, habiéndose utilizado las captaciones del mismo para la sanción disciplinaria del reclamante y el despido de otro trabajador de la entidad. Esta acción la considera totalmente desmedida y contraria al principio de proporcionalidad.

La parte reclamada, por su parte, manifiesta que los trabajadores son informados, desde la firma del contrato de trabajo, de la existencia del sistema de videocámaras, que carece de grabación de sonido.

A tenor del art. 20 del Estatuto de los Trabajadores “*Dirección y control de la actividad laboral*”, en su punto 3:

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

VILLA DE PINTO, S.L tuvo conocimiento del comportamiento inadecuado por parte del trabajador posteriormente sancionado y realizó la comprobación de la veracidad de los hechos mediante el visionado de las cámaras.

De la misma forma, VILLA DE PINTO, S.L, para proceder al despido de un trabajador, recurrió al visionado de las cámaras para comprobar la veracidad de las quejas recibidas por parte de compañeros y clientes.

IV

Información que deberá facilitarse cuando los datos personales se obtengan del interesado

El artículo 13 del RGPD establece que:

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

En relación con este artículo 13, VILLA DE PINTO, S.L., manifiesta que en el contrato de trabajo de sus empleados, en su cláusula cuarta, se informa al trabajador de la existencia de cámaras de seguridad.

V

Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

El artículo 89 de la LOPDGDD regula el *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo*:

1. Los empleadores podrán 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. Los empleadores habrán de informar con carácter previo, y de forma expresa,

clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

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.

La parte reclamante afirma que el sistema de videovigilancia instalado capta grabación de sonidos, motivo por el cual se produjo el despido del trabajador. En el anexo presentado junto a la reclamación relativo a este despido, se reproduce literalmente un fragmento de la conversación mantenida entre el trabajador y el cliente que realizó la queja a la dirección de la empresa.

VILLA DE PINTO, S.L manifiesta que todos los sistemas de video vigilancia implantados en el establecimiento se realizan sin grabación de sonido ya que el circuito cerrado de TV carece de sonido y en las cámaras de acceso remoto está deshabilitada la opción de sonido desde su instalación por lo que si tuvo conocimiento del contenido de la conversación entre cliente y trabajador fue por la queja interpuesta por ese cliente habitual.

VII

Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **VILLA DE PINTO, S.L.** y a la parte reclamante.

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 según lo preceptuado por el art. 114.1.c) de la LPACAP y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley, 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.

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