- **Expediente N.º: EXP202501663**

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: La Agencia Española de Protección de Datos ha tenido conocimiento a través de denuncia presentada por la JEFATURA SUPERIOR DE POLICÍA DE ***ÁREA.1***, de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos.

Con fecha 5 de febrero de 2025, la AEPD acuerda iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) para investigar a **EL CORTE INGLÉS, S.A.** con NIF **A28017895** (en adelante, ECI) y **SECURITAS SEGURIDAD ESPAÑA, S.A** con NIF **A28986800** (en adelante, SERVISECURITAS) en relación con los siguientes hechos:

En una inspección realizada el 13 de enero de 2025 por la policía nacional en el establecimiento de ECI ubicado en la plaza del ******DIRECCIÓN.1*** se encontraron dos archivadores que contenían imágenes extraídas del sistema de videovigilancia, tanto del mencionado establecimiento, como del supermercado anexo de la calle ******DIRECCIÓN.2***. Los archivadores también contenían imágenes correspondientes a otros dos establecimientos de ECI ubicados en ***(…).***

Los álbumes ***(…)*** contenían imágenes de personas, además de, en algunos casos, nombres y apellidos, así como una frase indicando la supuesta conducta sospechosa (supuestos hurtos, sustracciones) que habría llevado a la extracción de su fotograma del sistema de videovigilancia y posterior inclusión en el archivador, así como la fecha.

Los mencionados álbumes en el momento de la inspección estaban siendo visualizados por tres empleadas de SERVISECURITAS en las dependencias del Departamento de Seguridad del ECI ubicado en la ******DIRECCIÓN.1,*** lo que, de acuerdo con la policía nacional implica que la finalidad de los álbumes era "*la difusión entre los empleados del establecimiento (ya sea personal de seguridad o no, como así ocurrió al momento de la inspección, cuando personal auxiliar fue sorprendido visionándolos) para ponerlos sobre aviso y someter a estas personas a una vigilancia o seguimiento especial en caso de que accediesen al establecimiento".*

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el

artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD.

En el marco de las actuaciones previas de investigación se tuvo conocimiento de los siguientes aspectos a raíz de los escritos de contestación y documentación aportada por ECI (de 2 de junio de 2025 y 6 de abril de 2026) y SERVISECURITAS (de 12 de diciembre de 2025) como consecuencia de los requerimientos de información realizados:

- ECI es el responsable del tratamiento de las imágenes captadas por el sistema de videovigilancia del establecimiento ***(…).*** *A*segura que únicamente se realizan extracciones de imágenes *cuando procede*, *para su puesta a disposición de las autoridades pertinentes o, en su caso, a cualquier otro destinatario legitimado*.

- La prestación de servicios de seguridad y control de accesos se realiza ***(…)*** entidad distinta de SERVICIOS SECURITAS S.A. (conocida como SERVISECURITAS) que está contratada por ECI en el establecimiento ******DIRECCIÓN.1,*** para prestar servicios auxiliares. Entre las funciones de esta última no se prevé que tengan acceso alguno al sistema de videovigilancia ni al visionado de imágenes. El personal auxiliar desarrolla funciones destinadas a la orientación y apoyo a los clientes y usuarios que acceden al centro, pero que no se corresponden con funciones de seguridad y que no deberían implicar el tratamiento de datos personales. En concreto, en el contrato que rige la relación entre las partes se señala: ***"(…)".***

  Por otra parte, en los establecimientos de ***(…)*** es ******EMPRESA.1*** la entidad que presta servicios de videovigilancia para comprobar el estado de las instalaciones y garantizar la seguridad y protección de las personas y los bienes. Asimismo, ******EMPRESA.1*** presta otros servicios adicionales en estos centros, como el control de accesos a edificios e instalaciones, como encargado de tratamiento de ECI.

- ECI niega haber tenido conocimiento de los hechos hasta la llegada del requerimiento de la AEPD, reconoce la existencia de los álbumes que contenían imágenes de clientes extraídas del sistema de videovigilancia y niega su responsabilidad asegurando que la actuación fue realizada por propia iniciativa por un empleado ***(…)*** que habría actuado en contra de las políticas de la compañía. Insiste, asimismo, que el personal de SERVISECURITAS no tendría que haber accedido a las imágenes.

  Señala que su política de videovigilancia prohíbe la extracción de grabaciones salvo a los Delegados de Seguridad cuando existieran "*incidencias, sospechas o hechos delictivos, con el fin de bloquear las imágenes, conservándose únicamente a disposición de las Fuerzas y Cuerpos de Seguridad, Jueces y Tribunales"* y asegura que esta se

traslada "*internamente a todo el personal componente de esta área (Prevención y Seguridad) para la oportuna aplicación de la misma, incluidos los Delegados de Seguridad de la Compañía y se completa con las diferentes instrucciones y políticas específicas que emite la Dirección de Prevención y Seguridad Corporativa".* Remite copia de diferentes circulares anteriores a enero de 2025, así como el protocolo de extracción de imágenes para su remisión a sujetos legitimados. Por último, niega que situaciones similares se hayan producido en otros de sus centros.

- En relación con los logs del sistema de videovigilancia ECI, en el escrito de respuesta de 7 de agosto de 2025, afirma que no dispone de logs correspondientes a las fechas en que se produjo la extracción de las imágenes (correspondientes al período del 17 de junio de 2024 al 11 de enero de 2025) que se incluyen en los álbumes objeto de las presentes actuaciones de investigación, al no haberle resultado posible su recuperación dado que el sistema utilizado tiene una capacidad de almacenamiento limitada y sobre escribe al alcanzar el máximo de su capacidad.

  No obstante, cabe señalar que, según su propia manifestación, ECI tuvo conocimiento inicial de la inspección policial en la que se intervinieron los álbumes el 13 de enero de 2025, a través del propio Delegado de Seguridad ***A.A.A.*** y con acceso al acta de inspección emitida por la Dirección General de la Policía. Adicionalmente, con fecha 30 de abril de 2025, tuvo conocimiento de la denuncia interpuesta por la Dirección General de Policía ante esta Agencia. No consta si los logs del sistema de videovigilancia que permiten identificar a los usuarios que extrajeron las imágenes incluidas en los álbumes fueron consultados y verificados por ECI en algún momento previo al requerimiento de esta Agencia o si, en caso de haberlo sido, ya se habían sobrescrito. Posteriormente señala que las extracciones fueron realizadas por los ***(…).***

- Asimismo, en tanto que imágenes tomadas en diferentes establecimientos se encontraban en los archivadores, ECI asegura que no existe una compartición de álbumes entre centros, porque estos no se elaboran pero reconoce que *"para casos de robos o acciones delictivas de especial trascendencia (por ejemplo, actuaciones de bandas organizadas, reiteración de las acciones en distintos centros por delincuentes "itinerantes", casos de delincuencia transnacional organizada, etc.) al margen de las denuncias oportunas, se trasciende información a los centros de la organización con el único fin de prevenir los posibles actos ilícitos en los centros de la organización. Estas imágenes no se comunican a terceras compañías y solo tienen acceso a las mismas el personal de seguridad.*
  A modo de ejemplo de situaciones en las que se comparten imágenes entre centros, con el único fin de tratar de garantizar la seguridad en los mismos, se adjunta como Anexo 2 un correo electrónico recibido de la Jefatura Superior de la Policía de Aragón solicitando la cooperación en el resto del territorio. Por razones obvias, resulta necesario compartir

esta información con el personal de seguridad de otros centros ya que, si no, la petición de la Jefatura de Aragón y el fin perseguido resultarían inútiles.
Huelga decir que en ningún caso se justifica la extracción de las imágenes para cualquier otro fin (…)".

- ECI, en el escrito de respuesta de 7 de agosto de 2025, identifica a los usuarios de los establecimientos ECI de ***(…)*** que pueden acceder a las grabaciones del sistema de videovigilancia y descargar o exportar imágenes, correspondiéndose con los Delegados de Seguridad. Asimismo, asegura que:

(…).
(…):
- o ***(…).***
- o ***(…).***
- o ***(…).***
- o ***(…).***

- Señala, asimismo, que el proceso de extracción de imágenes permitido por ECI, negando que el ocurrido en ***(…),*** lo siguiente*:* ***(…).***
"(…).
(…):
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***
  - o ***(…).***

(…).
(…).
(…).
(…).
(…)".

- Por su parte, SERVISECURITAS identifica a las empleadas que fueron sorprendidas por los agentes visionando los álbumes de fotografías de clientes del establecimiento ECI ubicado en ******DIRECCIÓN.1,*** quienes aseguraron que era la primera vez que accedían a los álbumes, e insiste en que desconocía la existencia de estas prácticas, subrayando que estas empleadas no deberían haber accedido a las imágenes contenidas en los álbumes en cuestión.

- En relación con las medidas adoptadas a raíz de los hechos acontecidos:

a. SERVISECURITAS apunta a un refuerzo del mensaje dirigido al personal insistiendo en que los servicios prestados por SERVISECURITAS a ECI, y en concreto, las funciones que desempeñan las trabajadoras de SERVISECURITAS para ECI, no deben conllevar un tratamiento de datos personales. En particular se señala que "***(…)".***

b. Por su parte, ECI señala lo siguiente en su escrito de 2 de junio de 2025:

- *(…)* ***(…).*** *Al estar los Álbumes en custodia de la Jefatura, no se ha podido proceder a su inmediata supresión, sin perjuicio de que desde ECI no hay ninguna objeción a que la Jefatura proceda a su borrado y destrucción.*
- *Se ha abierto investigación interna para determinar el alcance de la actuación desarrollada en el centro de* ******DIRECCIÓN.1****, extendiendo la misma a todos los centros de la compañía. A día de hoy y siguiendo con el programa de auditoría de centros de seguridad implantado por El Corte Inglés (revisando más de 40 centros en 2024, así como 21 en 2025 antes de la recepción del requerimiento de esta Agencia), además del centro* ******DIRECCIÓN.1****, se han auditado otros* ***(…)****. A fecha de hoy, no consta que práctica similar se haya llevado a cabo por otros centros.*
- *Se remite circular desde la Dirección de Prevención y Seguridad Corporativa a los delegados de Seguridad recordando circulares previas sobre la diligente gestión de los accesos y custodia de imágenes. Además, merece la pena destacar que durante los años previos se han ido remitiendo distintas circulares sobre las obligaciones principales de videovigilancia y la protección de datos (e.g. proceso de extracción, principales obligaciones, casos relevantes de malas prácticas, etc.).*
- *Aprovechando el traslado del acta de la reunión de delegados regionales de seguridad de los pasados días 9 y 10, en la que se presentó la nueva guía de uso de videocámaras de la AEPD, se refuerza el mensaje sobre los principales aspectos referidos en la misma y su conservación. Cabe destacar que el año pasado se analizó el ejercicio de derechos en relación con la videovigilancia.*
- *Se procede a revisar el registro de tratamiento, análisis de riesgo y evaluación de impacto de los tratamientos.*
- *Se está preparando una acción formativa de refuerzo para los implicados en el tratamiento.*

Por otra parte, en su escrito de 4 de agosto de 2025 añade:

- *Los centros que han sido auditados con posterioridad a la respuesta al primer requerimiento (de la AEPD en el marco de las presentes actuaciones de investigación) han sido 5 centros de (…) y 5 centros en (…). A fecha de hoy, no consta que práctica similar a la que motivó la denuncia (…).*
- *Se han previsto en el plan de formación 2025/2026 acciones específicas en relación con la videovigilancia y el tratamiento de imágenes como refuerzo a la formación ya existente.*

Asimismo, ECI en el escrito de respuesta fechado el 6 de abril de 2026 añade:

- *El 3 de junio de 2025 se comunicó al* ******PUESTO.1*** *la medida disciplinaria impuesta (i.e., suspensión de empleo y sueldo por falta muy grave).* Por otra parte, señala que no se ha iniciado ***(…).***

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia 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 regirán 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
Licitud del tratamiento

El primer apartado del artículo 6 del RGPD establece lo siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del

interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

III
Conclusión

En el presente caso, los hechos que impulsaron el inicio de actuaciones previas de investigación conforme al artículo 67 de la LOPDGDD, tras la recepción de una denuncia de la Jefatura Superior de Policía de ***ÁREA.1*** se referían a la existencia de dos archivadores en un establecimiento del ECI en los que se recogían imágenes extraídas de los sistemas de videovigilancia de personas, así como a su visualización por personal auxiliar de SERVISECURITAS. Lo anterior denotaría carencias desde la perspectiva de protección de datos ligadas a la licitud de los tratamientos.

No obstante, durante las actuaciones previas de investigación se ha comprobado que los hechos constituían una práctica aislada no extendida a otros centros, además de la adopción de medidas por las entidades denunciadas para evitar actuaciones similares en un futuro.

Por un lado, SERVISECURITAS ha reforzado las instrucciones a su personal, modificando su Manual de Normas Básicas para insistir en que las funciones de su personal no deberían conllevar el tratamiento de datos personales.

Por otro lado, ECI ha acreditado haber remitido circulares de seguridad en las que se hacía referencia expresa a la prohibición de prácticas como las acontecidas, además de reforzar su plan de formación específico en materia de videovigilancia. Por otra parte, ha ratificado que su sistema general de grabación de imágenes cumple con las políticas de supresión automatizada en el plazo máximo de un mes establecido por la normativa vigente y ha impuesto ***(…).***

La reciente STJUE de 26 de septiembre de 2024, en el asunto C-768/2021, señala (el subrayado es de la AEPD):

"37 A este respecto, ha de señalarse que el RGPD deja a la autoridad de control un margen de apreciación en cuanto a la manera en que debe subsanar la deficiencia constatada, puesto que el artículo 58, apartado 2, del mismo confiere a dicha autoridad la facultad de adoptar diversas medidas correctoras. Así, el Tribunal de Justicia ya ha declarado que la elección del medio adecuado y necesario corresponde a la autoridad de control, que debe realizar tal elección tomando en consideración todas las circunstancias del caso concreto y cumpliendo con toda la diligencia requerida su misión consistente en velar por el pleno respeto del RGPD (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 112).
38 Sin embargo, este margen de apreciación está limitado por la necesidad de garantizar un nivel coherente y elevado de protección de los datos personales

mediante una aplicación rigurosa de las normas, como se desprende de los considerandos 7 y 10 del RGPD

…

41 En consecuencia, no puede deducirse ni del artículo 58, apartado 2, del RGPD ni del artículo 83 de este la existencia de una obligación a cargo de la autoridad de control de adoptar, en todos los casos, cuando constate una violación de la seguridad de datos personales, una medida correctora, en particular una multa administrativa, siendo su obligación, en tales circunstancias, reaccionar adecuadamente para subsanar la deficiencia constatada. (…) En estas circunstancias, como señaló el Abogado General en el punto 81 de sus conclusiones, el autor de una reclamación cuyos derechos han sido vulnerados no dispone de un derecho subjetivo a que la autoridad de control imponga una multa administrativa al responsable del tratamiento.

(…)

43 A este respecto, no se excluye que, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, la autoridad de control pueda abstenerse de adoptar una medida correctora aunque se haya constatado una violación de la seguridad de datos personales. Tal puede ser el caso, en particular, cuando la violación constatada no haya persistido, por ejemplo cuando el responsable del tratamiento, que, en principio, había aplicado medidas técnicas y organizativas apropiadas en el sentido del artículo 24 del RGPD, haya adoptado, tan pronto como haya tenido conocimiento de dicha violación, las medidas adecuadas y necesarias para que la violación finalice y no vuelva a producirse, habida cuenta de las obligaciones que le incumben, en particular, en virtud de los artículos 5, apartado 2, y 24 del mencionado Reglamento.

44 La interpretación según la cual la autoridad de control, cuando constata una violación de la seguridad de datos personales, no está obligada a adoptar en todos los casos una medida correctora con arreglo al artículo 58, apartado 2, del RGPD se ve corroborada por los objetivos perseguidos por este artículo 58, apartado 2, y por el artículo 83 de dicho Reglamento, respectivamente.

45 Por lo que respecta al objetivo perseguido por el artículo 58, apartado 2, del RGPD, del considerando 129 de este se desprende que esta disposición tiene por objeto garantizar la conformidad del tratamiento de datos personales con dicho Reglamento y la regularización de las situaciones de incumplimiento de este para que se ajusten al Derecho de la Unión, mediante la intervención de las autoridades de control nacionales (sentencia de 14 de marzo de 2024, Újpesti Polgármesteri Hivatal, C-46/23, EU:C:2024:239, apartado 40).

46 De lo anterior se infiere que la adopción de una medida correctora puede, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, no imponerse, siempre que la situación de infracción del RGPD ya haya sido subsanada y que se garantice la conformidad de los tratamientos de datos personales con dicho Reglamento por su responsable y que tal abstención de la autoridad de control no menoscabe la exigencia de una aplicación rigurosa de las normas, tal como se ha recordado en el apartado 38 de la presente sentencia."

El TJUE incide, por tanto, en el margen de apreciación que tienen las autoridades de control para, en el ejercicio de sus funciones, desarrollar y optar entre los poderes atribuidos por el artículo 58 del RGPD, teniendo en cuenta las circunstancias del caso concreto, así como velando por el pleno respeto del RGPD. La consigna que debe regir siempre la actuación de una autoridad de control es asegurar un nivel alto de protección de los datos personales.

Así, cabe que, aun cuando se hubiera constatado o se tuvieran indicios de que se ha producido una vulneración en materia de protección de datos, las autoridades de control se abstengan de ejercitar sus poderes correctivos cuando esta presunta infracción hubiera sido subsanada y se garantice la conformidad de los tratamientos de datos personales con el RGPD.

Lo señalado por el TJUE en la sentencia antes citada, refuerza la idea de proporcionalidad de actuación de las autoridades de control que se recoge, con anterioridad a que fuera dictada la mencionada sentencia, en los artículos 65.4 y 65.6 de la LOPDGDD, por los que se permite a la AEPD, en atención a las circunstancias del caso concreto, la inadmisión a trámite o el archivo de reclamaciones, cuando, tras el traslado de las mismas al responsable del tratamiento, este demostrara haber adoptado medidas para el cumplimiento de la normativa aplicable.

En consecuencia, de conformidad con la STJUE de 26 de septiembre de 2024, en el asunto C-768/2021 y atendiendo a las singulares circunstancias que conforman este caso, esta Agencia considera que no procede el despliegue de sus poderes correctivos previstos en el artículo 58 del RGPD.

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.

Por lo tanto, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **EL CORTE INGLÉS, S.A y SECURITAS SEGURIDAD ESPAÑA, S.A.**

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará 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 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia 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.

940-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos