- **Expediente N.º: EXP202412702**

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 tuvo conocimiento, a través de una denuncia, de ciertos hechos que podrían vulnerar la normativa en materia de protección de datos.

Con fecha 20 de junio de 2024, la Presidencia de la Agencia Española de Protección de Datos (AEPD) instó a la Subdirección General de Inspección de Datos (SGID) a 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 DILCAR GESTIÓN, S.L., con NIF B22339774 (en adelante, DILCAR), en relación con los siguientes hechos:

La indebida utilización de los medios técnicos puestos a disposición por parte del Ayuntamiento de Huesca a un concejal (en concreto, impresora y dirección de correo electrónico del grupo municipal al que pertenecía) para el desarrollo de su actividad profesional privada en la empresa DILCAR, con afectación a datos personales de sus clientes.

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 ha tenido conocimiento de los siguientes hechos:

- ***A.A.A.*** fue concejal del Ayuntamiento de Huesca adscrito al ***(…).*** A partir de ***(…)*** pasó a ser *(…)*. Compaginaba su labor como concejal con el desarrollo de su actividad profesional, ***(…)*** empresa DILCAR.

- Entre junio de 2019 y junio de 2023 era la única persona con acceso a la dirección de correo electrónico adscrita al ***(…).*** A partir de julio de 2023 pasaron a tener acceso dos personas más. En noviembre de 2023 ***A.A.A.*** deja de tener

acceso a la mencionada dirección de correo electrónico al dejar de estar vinculado al mencionado grupo municipal.

- El 29 de noviembre de 2022 consta el reenvío de un correo electrónico desde la dirección ******EMAIL.1*** a la dirección de correo electrónico del ***(…)*** que contiene datos personales de un cliente de DILCAR. Lo mismo ocurre el 25 de abril de 2023. Asimismo, el 20 de febrero de 2023 ***A.A.A.*** utilizó la impresora del Ayuntamiento para escanear documentación relativa a DILCAR en la que constaban datos personales de 4 clientes. Posteriormente remitió esa documentación desde la dirección de correo electrónico del ***(…)*** a la dirección de DILCAR.

- La utilización de las direcciones de correo vinculadas al Ayuntamiento para fines no relacionados con la actividad en el propio Ayuntamiento contraviene los protocolos y reglamentos de esta entidad. Constan recordatorios generales a todo el personal y miembros del consistorio sobre el uso del correo electrónico, al menos, los días 30 de abril de 2020 y 28 de septiembre de 2021. Además, el Pleno del Ayuntamiento adoptó por unanimidad el "Reglamento del uso de los recursos y accesos a los sistemas de información del Ayuntamiento de Huesca". El documento, entre otros extremos, prevé la prohibición general de cualquier uso personal del correo electrónico u otros canales de comunicación corporativos.

- DILCAR señala que la utilización de la dirección de correo electrónico del grupo municipal para el reenvío de documentación que contenía datos de sus clientes se llevó a cabo únicamente en tres ocasiones, que califica de aisladas y puntuales, y como consecuencia de una avería en la impresora de DILCAR.

- A raíz de lo ocurrido señala haber adoptado "*con carácter urgente, todas las medidas tendentes a la corrección de la concreta incidencia objeto de reclamación"*: el registro interno del incidente, la contratación de una consulta externa de protección de datos y la realización de una auditoría de protección de datos para actualizar e implantar medidas técnicas y organizativas necesarias en la entidad.

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

Seguridad del tratamiento

El artículo 32 del RGPD establece lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

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 por la AEPD- se referían a la utilización por parte del administrador de DILCAR, en su condición de concejal del Ayuntamiento de Huesca adscrito al ***(…)***, de la cuenta de correo electrónico ***(…)*** para el desarrollo de su actividad profesional.

En particular, se denunciaba la utilización de dicha cuenta para para el envío y recepción de documentación relativa a DILCAR, que contenía, en algunos casos, datos personales de sus clientes.

Durante las actuaciones previas de investigación se ha constatado la existencia de intercambios de correos entre la cuenta del grupo municipal y la cuenta corporativa de la empresa los días 29 de noviembre de 2022, 20 de febrero de 2023 y 25 de abril de 2023.

En el momento de producirse esos correos, no obstante, la única persona que tenía acceso a las cuenta de correo del grupo municipal era ***A.A.A.***, autor de los envíos, aun cuando la responsabilidad desde la perspectiva de protección de datos recaiga en DILCAR, y sin perjuicio de que, con posterioridad (a partir de noviembre de 2023) tuvieran acceso a esa dirección de correo electrónico otras dos personas (sujetas, por otra parte, a un deber de confidencialidad en relación con el tratamiento de datos personales impuesto por el propio Ayuntamiento).

A raíz de los hechos anteriores, DILCAR ha contratado a una empresa especializada en la prestación de servicios de consultoría y auditoría en materia de protección de datos, a los efectos de poner en práctica medidas efectivas para dar cumplimiento a la normativa sobre protección de datos.

Teniendo en cuenta todos los elementos expuestos, resulta procedente tomar en consideración la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 24 de septiembre de 2024, dictada en el asunto C 768/21, analiza un supuesto de brecha de datos personales en el que una autoridad de control (el Comisionado para la Protección de Datos y la Libertad de Información del Estado Federado de Hesse, Alemania) decidió no imponer sanción atendiendo a las circunstancias del caso concreto. En la sentencia se afirma lo siguiente:

"*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 24 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.

Así pues, 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 DILCAR GESTIÓN, S.L.

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