NOTA INFORMATIVA

La vulneración del deber de confidencialidad en la tramitación de expedientes de acoso laboral: un análisis desde la perspectiva de protección de datos

La Agencia Española de Protección de Datos (en adelante, la "**AEPD**") ha examinado recientemente, en su Resolución del Expediente nº EXP202411409 (en adelante, la "**Resolución**"), la actuación de una empresa que, **en el marco de un procedimiento interno por presunto acoso laboral, comunicó diversas resoluciones identificando expresamente a las personas denunciantes y denunciadas**. Esta forma de proceder permitió que varios destinatarios accedieran a información personal especialmente sensible, directamente vinculada a la intervención de dichas personas en un proceso de esta naturaleza.

En su resolución, **la AEPD concluye que tal actuación constituye una vulneración del deber de confidencialidad** previsto en la normativa de protección de datos, al implicar una divulgación injustificada y no necesaria de datos personales. Asimismo, recuerda que, incluso en el ámbito laboral, **las organizaciones deben extremar la diligencia en el tratamiento de la información relativa a investigaciones internas**, garantizando que su conocimiento se limite de forma estricta a quienes resulten indispensables para la tramitación del procedimiento.

Puntos clave a destacar

- La Resolución subraya que **el deber de confidencialidad constituye una obligación activa y permanente del responsable del tratamiento**. El hecho de que las personas implicadas en un procedimiento de acoso puedan conocer —o incluso inferir— la identidad de denunciantes y denunciados no legitima la divulgación indiscriminada de dicha información en resoluciones o comunicaciones internas. **La empresa debe adoptar medidas que eviten cualquier difusión innecesaria de datos personales**.

- **La identificación expresa de las personas denunciantes y denunciadas en procedimientos de acoso exige un estándar reforzado de diligencia, dado que se trata de información particularmente sensible en el contexto laboral**. Facilitar su acceso a terceros no estrictamente necesarios para la tramitación del expediente **contraviene el principio de confidencialidad y el de minimización** de datos establecidos por el RGPD, al implicar un tratamiento excesivo e injustificado.

1. Puntos claves de la sentencia

La Resolución analiza el **principio de confidencialidad** que toda empresa debe garantizar en el tratamiento de los datos personales de sus empleados, especialmente en el marco de los procedimientos tramitados a través del **canal interno de denuncias**.

En el caso examinado, la reclamante —una de las personas afectadas— denunció que la empresa hizo pública su condición de denunciante en un procedimiento de acoso laboral, divulgando además su nombre y apellidos. En total, **15 personas** resultaron afectadas por el incidente: **5 denunciantes y 10 denunciados**.

La AEPD estima la reclamación y concluye que la empresa vulneró el **principio de integridad y confidencialidad** recogido en el artículo 5.1.f) del RGPD, al permitir un acceso innecesario y generalizado a datos personales de denunciantes y denunciados, sin aplicar las medidas técnicas y organizativas apropiadas para garantizar su protección. Conforme destaca la Resolución, el responsable del tratamiento estaba obligado a extremar la diligencia en este tipo de procedimientos, lo que no ocurrió en el caso analizado.

En particular, la AEPD pone de relieve los siguientes aspectos:

- **La comunicación de resoluciones debe preservar el anonimato de las personas afectadas.** La identificación expresa de denunciantes y denunciados en comunicaciones internas expone información especialmente sensible y facilita un acceso indiscriminado a datos personales, vulnerando así el deber de confidencialidad y el principio de minimización.

- **La existencia de protocolos internos no justifica la pérdida de confidencialidad.** La Agencia rechaza el argumento de que no existía una "posibilidad real de desconocimiento" entre las personas implicadas. Recuerda que la obligación de confidencialidad es objetiva y no depende del grado de conocimiento previo entre los participantes, sino de que el responsable adopte medidas efectivas para evitar accesos innecesarios o comunicaciones indebidas.

- **Mayor diligencia en procedimientos de acoso y en el canal interno de denuncias.** La AEPD subraya que los datos tratados en este tipo de expedientes requieren un nivel especialmente reforzado de protección, exigiéndose al responsable una gestión particularmente prudente y restrictiva en relación con los destinatarios, el contenido y la forma de las comunicaciones.

2. Análisis de la normativa aplicable

La existencia de **sistemas internos de denuncias o *whistleblowing*** encuentra cobertura legal en el artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, la "**LOPDGDD**") así

como en la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

El tratamiento de datos personales derivado del funcionamiento de estos sistemas se ampara en la base jurídica del **interés público**, conforme al artículo 6.1.e) del Reglamento (UE) 2016/679 (en adelante, el "**RGPD**").

No obstante, que el tratamiento sea lícito no exime al responsable del tratamiento de garantizar el respeto absoluto a los principios fundamentales de la protección de datos, entre ellos los de minimización, confidencialidad, proporcionalidad y limitación del tratamiento.

Además, en esta línea, la Guía de la AEPD sobre protección de datos en las relaciones laborales establece criterios particularmente relevantes para los canales internos de denuncias y los procedimientos asociados —incluidos los de acoso laboral— que deben ser observados por los responsables del tratamiento.

Entre ellos, destacan los siguientes:

a) Principio de proporcionalidad y limitación del tratamiento:

Además del principio de integridad y confidencialidad, el tratamiento de datos personales en estos sistemas debe atender estrictamente a los principios de proporcionalidad y limitación del tratamiento.

Esto implica que las denuncias canalizadas a través del sistema deben restringirse a hechos que tengan incidencia real en la relación laboral o profesional, y que los datos recabados no puedan utilizarse para finalidades distintas de aquellas que justificaron la implantación del sistema. El incumplimiento de esta limitación constituiría un tratamiento excesivo o incompatible con los fines declarados.

b) Limitación del acceso a los datos personales:

La Guía de la AEPD delimita con claridad quiénes pueden acceder a la información gestionada a través del canal interno de denuncias. En concreto, el acceso debe limitarse exclusivamente a:

- el personal de control interno y cumplimiento, o
- el encargado del tratamiento designado por la organización.

Solo será lícito permitir el acceso a otras personas —o comunicar datos a terceros— cuando ello resulte estrictamente necesario para:

- adoptar medidas disciplinarias, o

- tramitar procedimientos judiciales o administrativos derivados de los hechos denunciados.

En cuanto al personal de recursos humanos, únicamente podrá acceder a estos datos cuando sea imprescindible para la gestión de un procedimiento disciplinario concreto.

Este criterio reafirma la necesidad de limitar al máximo los destinatarios de la información y de impedir accesos indiscriminados o comunicaciones innecesarias que puedan comprometer el principio de confidencialidad.

c) Plazos de conservación:

Los datos deben conservarse únicamente durante el tiempo imprescindible para la investigación de los hechos. Si la denuncia no diera lugar a actuaciones contra la persona denunciada, los datos deberán ser suprimidos.

Solo podrá mantenerse la información más allá de ese periodo cuando resulte necesaria para la adopción de medidas disciplinarias o la tramitación de procedimientos legales.

En todo caso, la AEPD establece que los datos deben eliminarse en un plazo máximo de tres meses desde su incorporación al sistema, sin obligación de bloqueo, salvo cuando deban conservarse exclusivamente para acreditar el adecuado funcionamiento del modelo de prevención de delitos.

Por último, las denuncias que no sean tramitadas únicamente podrán conservarse de forma anonimizada, de manera que no sea posible identificar a las personas implicadas.

3. Análisis-jurídico laboral

La Resolución pone de manifiesto una serie de incumplimientos con relevancia laboral que conviene destacar:

3.1. Incumplimiento del deber empresarial de protección en materia de seguridad y salud en el trabajo (arts. 14 y 15 LPRL)

La empresa tiene la obligación de garantizar la seguridad y salud de las personas trabajadoras, incluyendo la prevención de riesgos psicosociales.

La difusión de las identidades en un procedimiento de acoso:

- genera un entorno laboral hostil,
- compromete el bienestar de denunciantes y denunciados, y
- puede provocar daños psicológicos.

La difusión de las identidades en el expediente objeto de análisis derivó en consecuencias laborales concretas: una de las denunciantes sufrió un ataque de ansiedad deviniendo en baja médica el mismo día en que la información se hizo pública en el centro de trabajo.

Ello supone un incumplimiento del deber general de protección en materia de seguridad y salud en el trabajo.

3.2. Quiebra de la confidencialidad en procedimientos de acoso

Los procedimientos internos de investigación por acoso laboral exigen un tratamiento especialmente reservado de la información, dada la sensibilidad de los datos personales implicados y el impacto que su divulgación puede generar en las personas afectadas. La confidencialidad constituye, por tanto, un deber reforzado tanto para la empresa como para cualquier órgano o persona que intervenga en el proceso.

En el caso analizado, se constató una vulneración grave de este deber de confidencialidad debido a diversas actuaciones irregulares:

- La empresa difundió resoluciones relacionadas con el procedimiento de acoso a un total de 15 personas, incluyendo la identificación explícita de denunciantes y denunciados.
- El Comité de Empresa remitió documentación interna con información sensible a terceros, ampliando aún más el ámbito de la revelación indebida.
- Parte de la información terminó circulando en grupos de WhatsApp laborales, donde se produjeron incluso comentarios de desprecio hacia las personas implicadas.

Estos hechos revelan una quiebra sustancial del estándar de diligencia exigible en el ámbito laboral, especialmente porque la empresa disponía de protocolos formales que reconocían expresamente la obligación de confidencialidad, pero no adoptó medidas organizativas o técnicas que garantizaran su cumplimiento efectivo. La existencia de protocolos resulta insuficiente si no se acompañan de procedimientos adecuados para asegurar su aplicación.

La resolución subraya que el deber de confidencialidad en estos procesos no deriva únicamente de la normativa interna de la empresa, sino que tiene su fundamento directo en el Reglamento General de Protección de Datos (RGPD). En particular, conforme al artículo 83.2.a) del RGPD, la sensibilidad de los datos afectados y las circunstancias de su tratamiento exigen un nivel de protección especialmente riguroso por parte del responsable de tratamiento.

Atendiendo a la naturaleza de los datos revelados —la condición de denunciante o denunciado en un procedimiento de acoso laboral— y a las exigencias reforzadas de reserva que deben observarse en estos casos, la autoridad de control calificó el grado de negligencia como alto. La divulgación indebida no sólo comprometió la privacidad de las personas afectadas, sino que también agravó su exposición a posibles represalias o daños reputacionales, evidenciando la necesidad de reforzar las prácticas de protección de datos en el marco de los protocolos de acoso.

En paralelo a estas obligaciones en materia de protección de datos, el marco normativo laboral —particularmente los artículos 48 de la LO 3/2007 y 12 de la LO 10/2022— impone a todas las empresas, con independencia de su tamaño, la obligación de garantizar condiciones de trabajo que prevengan conductas contrarias a la libertad sexual y a la integridad moral. Ello incluye la implantación de un procedimiento específico de prevención y actuación frente al acoso, integrado por un protocolo preventivo y un procedimiento interno de investigación.

Estas medidas deben negociarse con la representación legal de las personas trabajadoras (RLPT), y cuando la empresa está obligada a contar con un plan de igualdad, su negociación se integra en el propio proceso del plan conforme al RD 901/2020. La LO 10/2022 refuerza además estas obligaciones al exigir formación, sensibilización y la inclusión de la violencia sexual en la evaluación de riesgos laborales, medidas que igualmente requieren negociación con la RLPT.

No obstante, aunque la RLPT desempeña un papel preventivo y de vigilancia del cumplimiento normativo (arts. 64.7 y 65 ET), su participación no alcanza a la instrucción de expedientes individuales de acoso. La normativa en igualdad le atribuye funciones de sensibilización y de comunicación a la dirección de aquellas conductas que puedan propiciar acoso (art. 48.2 LO 3/2007), pudiendo canalizar denuncias pero sin intervenir en la investigación de los hechos. Tampoco posee un derecho general de acceso a datos sensibles derivados de estos procedimientos, encontrándose además sometida al deber de sigilo. Su intervención en expedientes disciplinarios únicamente se activa cuando la persona afectada es representante de los trabajadores o está afiliada a un sindicato. De forma similar, en los sistemas internos de información regulados por la Ley 2/2023, la RLPT cuenta con facultades de consulta previa, asesoramiento y apoyo a las personas informantes, pero no con competencias de gestión ni de investigación.

En conjunto, la normativa articula un equilibrio claro: la RLPT tiene funciones preventivas, de apoyo y de canalización de denuncias, mientras que la empresa ostenta de manera exclusiva la competencia para instruir los expedientes y realizar las investigaciones internas. Esta exclusividad implica, a su vez, una especial responsabilidad en asegurar la confidencialidad y la adecuada protección de datos durante todo el proceso, reforzando la idea de que disponer de protocolos formales no basta si no van acompañados de mecanismos efectivos para garantizar su cumplimiento.

3.3. Riesgo de vulneración de derechos fundamentales

Las conductas descritas pueden suponer vulneración del derecho a:

- la intimidad,
- la dignidad e integridad moral,
- la indemnidad (al quedar expuesta la condición de las personas denunciantes).

Desde la perspectiva sancionadora, la Ley sobre Infracciones y Sanciones en el Orden Social (LISOS) tipifica como **infracción muy grave** los actos empresariales contrarios a la intimidad y dignidad de las personas trabajadoras, con multas que pueden oscilar entre **7.501 y 225.018 euros** (art. 40.1.c).

3.4. Necesidad de adoptar medidas correctoras

- Posible infracción y potestad de la AEPD

Si se confirma la vulneración del artículo 5.1.f) RGPD, la AEPD puede ordenar —según el artículo 58.2.d) RGPD— que el responsable implemente las medidas necesarias para adecuar el tratamiento a la normativa, especialmente en lo relativo a la confidencialidad.

La prevención del acoso, y su investigación interna, constituye una obligación normativa de la empresa que no puede quedar al arbitrio de terceras partes, constituyendo el acoso y la violencia sexual riesgos psicosociales cuya prevención forma parte de la gestión preventiva de la empresa.

Los incumplimientos de la empresa en materia de acoso, incluso la mera tolerancia, la falta de investigación o una investigación inadecuada, o la no adopción de las medidas necesarias para impedirlo, pueden constituir infracción muy grave por la LISOS, con sanciones de hasta 225.018 euros.

- Identificación de hechos y alcance de las medidas

La resolución detalla los hechos y la presunta infracción, de los que se deriva el alcance de las medidas correctoras. No obstante, corresponde únicamente al responsable definir los procedimientos concretos para aplicarlas, conforme a los principios de responsabilidad proactiva y enfoque basado en riesgos.

- Plazo para la adopción de medidas

Las medidas podrán exigirse con un **plazo máximo de tres meses** desde que la resolución sea ejecutiva. Esta obligación es compatible con la imposición de una sanción económica.

- Consecuencias del incumplimiento

El incumplimiento de la orden podrá constituir una nueva infracción conforme a los artículos 83.5 y 83.6 RGPD, pudiendo dar lugar a otro procedimiento sancionador. Ni el reconocimiento de la infracción ni el pago de la sanción eximen de implantar y acreditar ante la AEPD las medidas exigidas.

4. Conclusiones alcanzadas

En conclusión, la protección de los datos personales tratados en el marco de un canal interno de denuncias exige un **nivel reforzado de diligencia**, habida cuenta del carácter especialmente sensible de la información y de la relevancia de los intereses en juego.

Incluso en aquellos supuestos en los que pueda existir un conocimiento previo —o fácilmente deducible— de la identidad de las personas afectadas, la empresa **sigue obligada** a preservar de manera estricta la confidencialidad tanto de denunciantes como de denunciados, evitando cualquier acceso, comunicación o difusión que no resulte **estrictamente necesario** para la adecuada tramitación del procedimiento.

Este deber implica no solo el cumplimiento de las obligaciones generales previstas en el RGPD, sino también la observancia de los **criterios interpretativos fijados por la AEPD**, que exigen una limitación rigurosa de los accesos, una comunicación prudente y un tratamiento siempre proporcional al fin legítimo perseguido. En el caso analizado, ha quedado acreditado que la empresa no adoptó las medidas necesarias para garantizar la **confidencialidad e integridad** de los datos personales, permitiendo un acceso injustificado a información especialmente sensible en el contexto laboral.

Todo ello constituye una vulneración del **principio establecido en el artículo 5.1.f) del RGPD**, que impone al responsable del tratamiento la obligación de garantizar que los datos personales se traten de forma que se asegure su seguridad y se impidan accesos no autorizados o usos indebidos.

Por otro lado, desde una perspectiva jurídico-laboral, los hechos evidencian una serie de incumplimientos relevantes por parte de la empresa en relación con el deber de confidencialidad y la diligencia exigible en la gestión de los procedimientos de acoso laboral y del canal interno de denuncias.

La resolución pone de manifiesto que la normativa aplicable impone que los canales internos de información sean **confidenciales, seguros y accesibles**, garantizando que todas las personas puedan comunicar hechos objeto de denuncia sin temor a represalias. La reserva y el anonimato no solo constituyen elementos esenciales para fomentar la denuncia, sino que hoy representan un **requisito legal ineludible**.

Sin embargo, la empresa no adoptó las cautelas mínimas necesarias para proteger la información gestionada, comprometiendo así la privacidad de las personas afectadas y aumentando su exposición a riesgos como daños reputacionales, presiones internas o posibles represalias. Por ello, y con el fin de reforzar la seguridad jurídica en este ámbito, resulta recomendable implementar una serie de medidas prácticas orientadas a minimizar estos riesgos.

En conclusión, el caso analizado evidencia una **vulneración clara y grave** de las obligaciones empresariales en materia de protección de datos y prevención del acoso laboral. La actuación empresarial incumplió el deber de confidencialidad respecto de las personas implicadas, al no garantizar un tratamiento reservado, seguro y limitado de la información.

La **difusión indebida de datos personales especialmente sensibles**, la ausencia de medidas efectivas para prevenir accesos no autorizados y la deficiente gestión del canal

interno de denuncias revelan una quiebra sustancial del estándar de diligencia exigible en este ámbito.

Todo ello implica, como ha sido expuesto, la necesidad de adoptar medidas jurídicas, técnicas y organizativas que garanticen el cumplimiento normativo, así como la confidencialidad de la información, evitando que su transmisión a terceros no autorizados pueda ser considerado una brecha de seguridad o un incumplimiento en relación con el precepto reseñado.