

EL RGPD UE 2016/679 EN APLICACIÓN

El Delegado de protección de datos aliado estratégico en el cumplimiento normativo

La figura del Delegado de protección de datos (DPD) se consolida en el ordenamiento jurídico español como un pilar esencial del cumplimiento normativo en materia de protección de datos personales. La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), refuerza su relevancia, ampliando el alcance práctico de esta figura y adaptándola a la realidad de las entidades en el tratamiento de datos personales.

Debido a la creciente complejidad de los tratamientos, el uso intensivo de tecnologías digitales y al impacto que determinadas actividades pueden tener sobre los derechos y libertades de las personas, algunas organizaciones específicas precisan contar con un asesor especializado, independiente y con conocimientos jurídicos y técnicos suficientes para supervisar de forma continuada el cumplimiento de la normativa.

El Delegado de protección de datos facilita la implantación de políticas internas, la gestión de riesgos y la interlocución con la Agencia Española de Protección de Datos. Su presencia efectiva permite anticipar incumplimientos, reducir la exposición a sanciones y demostrar una verdadera cultura de protección de datos, alineada con las exigencias del marco normativo español y europeo.

Contenido

- 1.El Delegado de protección de datos aliado estratégico en el cumplimiento normativo.
- 2.Sancionada una entidad con 80.000€ por la cesión ilícita de datos de empleados a terceros y uso de su teléfono personal.
- 3.*Fingerprinting* o Huella digital del dispositivo (I).
- 4.La AEPD alerta sobre los riesgos visibles e invisibles del uso de imágenes de terceros en sistemas de inteligencia artificial.
- 5.Autenticación segura: el pilar esencial de la ciberseguridad en entornos digitales.



IMPORTANTE

No designar Delegado de Protección de Datos en supuestos obligatorios constituye una infracción grave del RGPD, sancionable con multas administrativas significativas.

SANCIONES DE LA AEPD

Sancionada una entidad con 80.000€ por la cesión ilícita de datos de empleados a terceros y uso de su teléfono personal

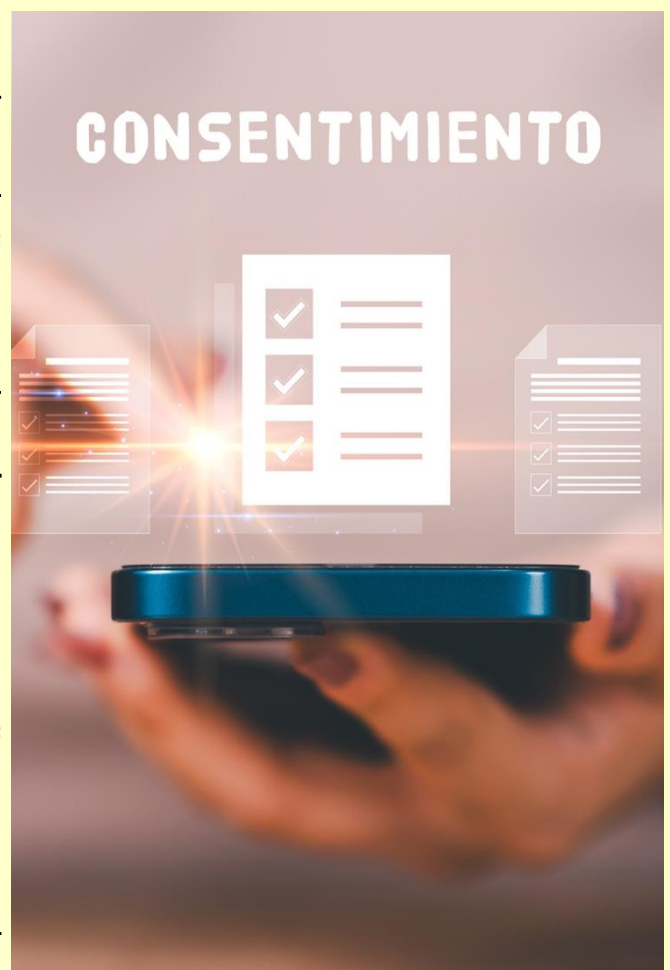
La Agencia Española de Protección de Datos, en su resolución [PS-00456-2025](#), sanciona a una entidad por la cesión ilícita de datos personales de los trabajadores/as sin legitimación adecuada ni alternativa al uso de su teléfono personal.

La denuncia fue formulada por la representación legal de los trabajadores, en concreto, se denunciaba que la entidad había solicitado al personal laboral sus números de teléfono móviles personales y otros datos identificativos, sin proporcionar información adecuada ni recabar consentimiento, para utilizarlos en el acceso a herramientas informáticas con la finalidad de doble factor de autenticación.

Los empleados comenzaron a recibir en sus teléfonos personales mensajes con credenciales de acceso a sistemas corporativos del cliente, deduciéndose que se habían comunicado dichos datos sin base jurídica válida y sin ofrecer alternativas menos intrusivas, como el uso de medios corporativos. Asimismo, se alegó la inexistencia de información clara sobre la transferencia internacional de datos y omitir el informe desfavorable del Delegado de Protección de Datos sobre esta práctica.

La Agencia concluyó que dicho tratamiento no era necesario para la ejecución del contrato laboral y que vulneraba el principio de licitud del artículo 5.1.a) del RGPD. La multa administrativa alcanzó los 80.000€.

El uso laboral del móvil personal exige consentimiento libre e informado del trabajador/a, facilitando alternativas e información previa.



IMPORTANTE

La conducta fue calificada como infracción muy grave, imponiéndose una sanción, junto con la obligación de cesar en el uso de teléfonos personales y adoptar medidas correctivas.

LA AEPD ACLARA***Fingerprinting* o Huella digital del dispositivo (I)**

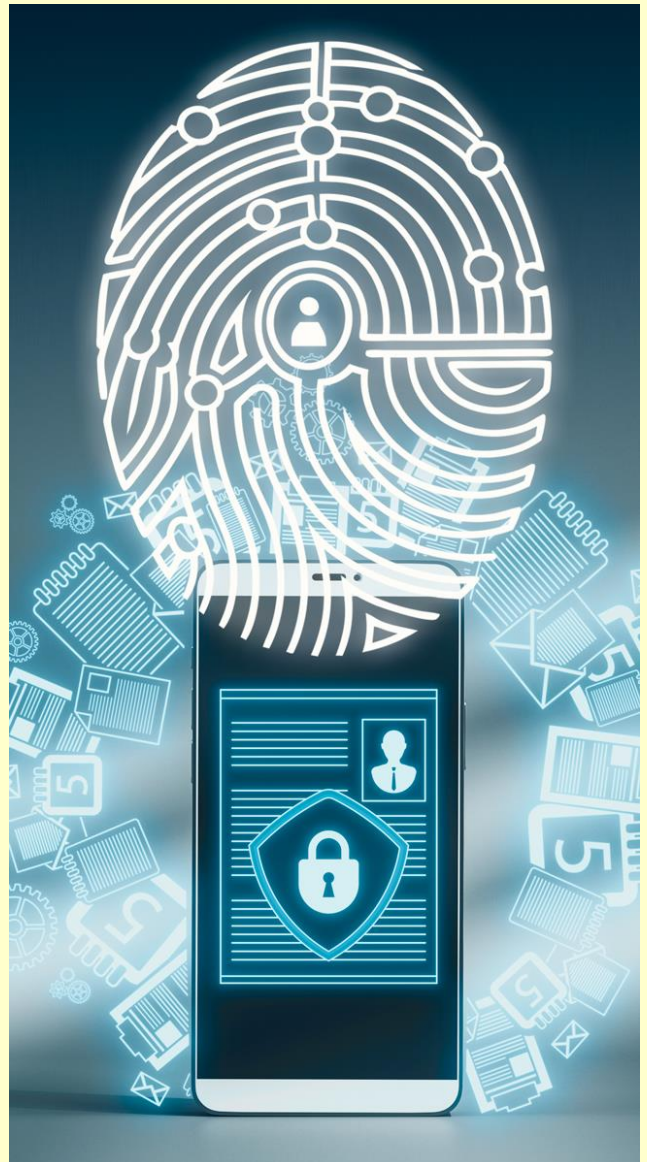
La Agencia Española de Protección de Datos en su espacio de áreas de actuación/Internet y nuevas tecnologías publica la guía de [*Fingerprinting* o Huella digital del dispositivo](#) en el que se realiza una aproximación al concepto de huella digital del dispositivo.

En el día de hoy los navegadores pueden ser configurados por el usuario, para que no acepten cookies o bien para que acepten cookies temporales que se borran automáticamente al cerrar el navegador. Sin embargo, existen nuevas formas de salvar las protecciones para recopilar y explotar datos de los usuarios.

Un ejemplo sencillo ayuda a entender su alcance: aunque dos personas utilicen el mismo navegador, pequeñas diferencias en la configuración de su dispositivo permiten distinguirlas con gran precisión. De este modo, incluso si el usuario borra cookies o navega en modo incógnito, puede seguir siendo reconocido.

El estudio de la AEPD demuestra que la recopilación de características técnicas del navegador y del equipo —resolución de pantalla, sistema operativo, fuentes instaladas o configuración gráfica— es posible construir un identificador prácticamente único.

Desde el punto de vista de la privacidad, el impacto es evidente. Identificar un dispositivo equivale, en la práctica, a identificar a la persona que lo utiliza.

**IMPORTANTE**

El usuario/a rara vez es consciente de que este tratamiento se está produciendo, lo que dificulta el ejercicio de sus derechos.

ACTUALIDAD CIBERSEGURIDAD Y PRIVACIDAD

La AEPD alerta sobre los riesgos visibles e invisibles del uso de imágenes de terceros en sistemas de inteligencia artificial

Fuente: [AEPD](#)

Madrid (13 de enero de 2026)

El primer apartado de la nota se centra en el impacto visible derivado de generar y difundir imágenes de terceros mediante IA. El documento presta especial atención a situaciones de alto riesgo, como la sexualización y el contenido íntimo sintético, la atribución de hechos no reales con efectos reputacionales, la descontextualización de las imágenes o la utilización de contenidos que afectan a menores de edad o personas en situación de especial vulnerabilidad.

El segundo apartado aborda los riesgos menos visibles, aquellos que se producen por el mero hecho de subir una imagen o un vídeo a un sistema de IA, aunque el resultado no se publique. Entre ellos, la Agencia destaca la pérdida efectiva de control sobre la imagen al intervenir un tercero tecnológico, la retención y la existencia de copias no visibles, la intervención de múltiples actores, la generación de metadatos o el riesgo de identificación persistente en sistemas capaces de reutilizar rasgos de una persona en múltiples contenidos.

Por último, la nota identifica las situaciones que suelen ser especialmente relevantes para la AEPD, aclarando los límites de la normativa de protección de datos, por ejemplo, en ámbitos personales o domésticos sin difusión más allá de ese entorno.

La Agencia presta especial atención a los supuestos en los que el uso de imágenes o vídeos de terceros mediante sistemas de inteligencia artificial incrementa de forma significativa los riesgos para la persona afectada. Esto ocurre, en particular, cuando se produce una pérdida efectiva de control sobre la propia imagen, se generan contenidos verosímiles que pueden atribuir a la persona hechos o conductas que no han ocurrido, se ven implicados menores de edad o personas especialmente vulnerables, se introducen elementos de sexualización, humillación o descrédito, o se difunden los contenidos en entornos en los que el impacto personal, social o profesional puede ser especialmente intenso.

La Agencia también añade que pueden verse afectados otros derechos fundamentales, como el honor, la intimidad o la propia imagen, y que resulten aplicables otras normas del ordenamiento jurídico, incluido el Código Penal. En caso de indicios claros de delito, la actuación correspondería a las autoridades policiales, la Fiscalía y, en su caso, los órganos judiciales, que son los competentes para la investigación y persecución penal de estos hechos.

Puede ver información relacionada en el siguiente enlace:

[El uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos visibles e invisibles.](#)

EL PROFESIONAL RESPONDE

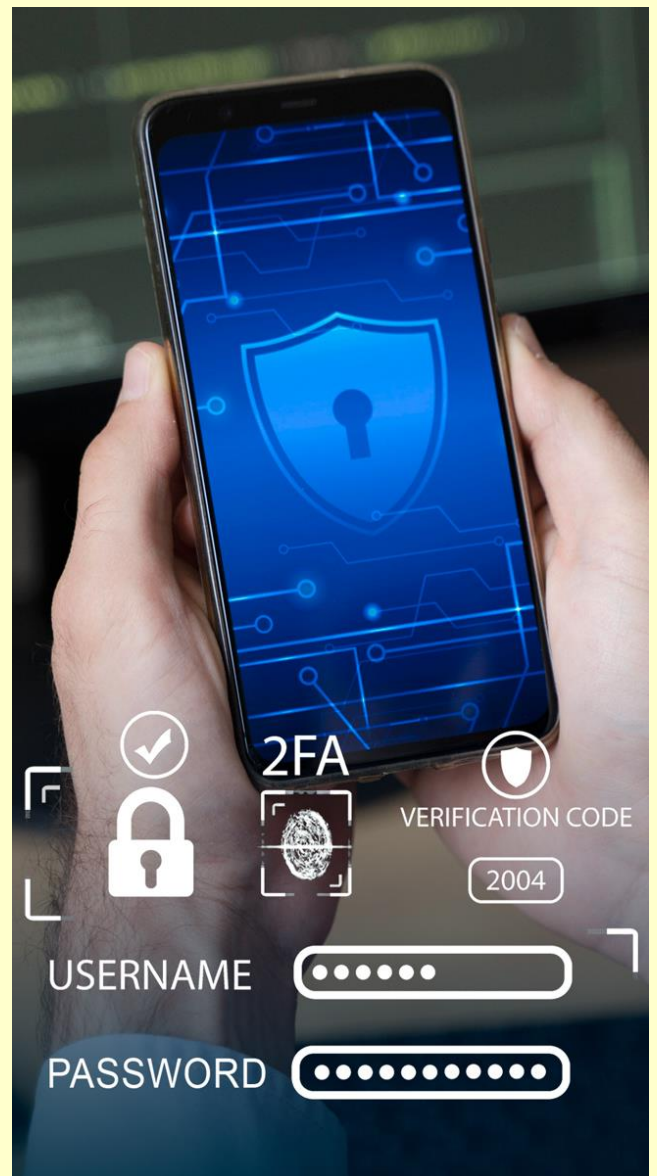
Autenticación segura: el pilar esencial de la ciberseguridad en entornos digitales

La autenticación segura es uno de los controles básicos y más críticos dentro de cualquier sistema de gestión de la seguridad de la información. Tanto la norma ISO 27001 como el Esquema Nacional de Seguridad (ENS) identifican el control de accesos como una medida esencial para garantizar que únicamente usuarios autorizados puedan interactuar con los sistemas y recursos de la organización.

Cuando hablamos de ciberseguridad, pocas medidas resultan tan determinantes —y a la vez tan infravaloradas— como la autenticación. Verificar correctamente quién accede a un sistema no es una cuestión accesorio, sino la primera barrera frente a la mayoría de los incidentes de seguridad que afectan hoy a organizaciones de cualquier tamaño.

La experiencia demuestra que un elevado porcentaje de incidentes de seguridad se produce por el uso de contraseñas débiles, reutilizadas o comprometidas, lo que evidencia la necesidad de implantar mecanismos de autenticación robustos y adaptados al riesgo.

Invertir en una autenticación robusta no solo reduce la probabilidad de accesos indebidos, sino que aporta estabilidad, confianza y continuidad operativa. Es, en definitiva, una decisión de madurez en la gestión de la ciberseguridad.



IMPORTANTE

No se trata únicamente de verificar quién accede, sino de hacerlo de forma fiable, trazable y resistente a ataques.