

### EL RGPD UE 2016/679 EN APLICACIÓN

## ¿Qué se considera una persona física identificada o identificable? (I)

Hoy en día la rápida evolución tecnológica y un mundo cada vez más globalizado plantean nuevos retos para la protección de los datos personales. La tecnología ha transformado la forma en que recopilamos, compartimos y utilizamos datos personales. Esta transformación ha traído consigo muchos beneficios, pero también plantea riesgos para nuestra privacidad.

El RGPD define en su artículo 4.1 *“datos personales”* como toda información sobre una persona física identificada o identificable, es decir sobre el interesado. La diferencia entre ambos términos es la siguiente:

- **Persona física identificada:** cuando la información claramente señala a una persona en particular. Por ejemplo, cuando tratamos los datos identificativos de una persona nombre y apellidos.
- **Persona física identificable:** A veces con información que tenemos por si sola no podemos identificar a la persona, pero si se combinan con otros datos, se puede averiguar su identidad. Por ejemplo, si tenemos un número de teléfono o una dirección IP, puede que no sepamos de inmediato a quién pertenece, pero con la información adicional adecuada, podemos identificar a esa persona.

#### Contenido

1. ¿Qué se considera una persona física identificada o identificable? (I).
2. Sancionada una microempresa de eventos por recoger datos excesivos y no informar debidamente.
3. La identidad como derecho.
4. La Agencia presenta un informe sobre la influencia de los patrones adictivos en Internet, y en especial sobre los menores.
5. ¿Cómo puedo proteger de los ciberataques los activos principales de mi empresa?



#### IMPORTANTE

El responsable del tratamiento debe informar al interesado sobre el uso y propósito del tratamiento de sus datos personales, garantizando transparencia y protección de la privacidad en todo momento.

## SANCIONES DE LA AEPD

### Sancionada una microempresa de eventos por recoger datos excesivos y no informar debidamente

En la resolución de la [AEPD](https://www.aepd.es/documento/ps-00570-2023.pdf) <https://www.aepd.es/documento/ps-00570-2023.pdf> se sanciona con 5.000€ a una microempresa de eventos por recoger datos excesivos y no informar debidamente en su política de privacidad.

La parte reclamante indica en su escrito de denuncia que, para asistir a los conciertos con menores, se requieren autorizaciones con copia del DNI y datos personales de los autorizantes y menores. Sin embargo, la política de privacidad de los formularios de la recogida de datos en la web no informa adecuadamente sobre la protección de datos.

La AEPD estimó que la empresa recogía datos excesivos al solicitar una fotocopia por ambas caras del DNI. Las categorías de datos recogidos deben ser los estrictamente necesarios para la finalidad del tratamiento. Además, en su página web no estaba informando debidamente sobre el tratamiento de los datos personales. La política de privacidad hacía referencia a la antigua Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de carácter Personal.

Junto con la sanción económica de 5.000€ se le impone a la entidad a que en el plazo de un mes adopte las medidas adecuadas para actualizar los textos a la normativa y elimine la recogida de la fotocopia del DNI en sus formularios.

La referencia a la antigua Ley Orgánica 15/1999 supone un incumplimiento del deber de informar por parte del responsable del tratamiento.



#### IMPORTANTE

El responsable del tratamiento permanecerá atento a los cambios durante de todo el ciclo de vida del tratamiento de los datos personales.

## LA AEPD ACLARA

### La identidad como derecho

En la página de la [AEPD](#) encontramos información relevante sobre aspectos de la privacidad. En este post la AEPD analiza las implicaciones de tratar la identidad como un servicio en lugar de como un derecho fundamental. Esto puede suponer un riesgo para los derechos y libertades de las personas, a la inclusión social y a la igualdad.

La identidad es un derecho fundamental reconocido internacionalmente en la Declaración Universal de Derechos Humanos. Sin identidad jurídica, se limitan la educación, el empleo, la atención médica, la protección social, los servicios financieros y el voto, entre otros derechos.

La identidad en España está garantizada en la Ley Orgánica de Protección de la Seguridad Ciudadana que regula la expedición del DNI. Este es el único documento con suficiente valor por sí solo para la acreditación de la identidad de los datos personales de su titular, tanto en el mundo físico como en el digital. La identidad de las personas no pertenece al Estado o a un tercero, sino a los ciudadanos.

Las iniciativas legislativas europeas como *eIDAS2* o la regulación de los pasaportes y documentos de viaje siguen el enfoque de la “**identidad como derecho**”. Estas normas europeas buscan estandarizar y mejorar la gestión de identidades, apoyando el acceso y la innovación.



#### IMPORTANTE

El RGPD resalta la importancia de proteger los datos de carácter personal para prevenir la usurpación de identidad y el fraude, garantizando la libertad y autonomía de las personas.

## ACTUALIDAD LOPD

La Agencia presenta un informe sobre la influencia de los patrones adictivos en Internet, y en especial sobre los menores



Fuente: [AEPD](#)

(10 de julio de 2024). La Agencia Española de Protección de Datos (AEPD) ha presentado [un informe](#) que analiza cómo los tratamientos de los datos personales de los usuarios en numerosas plataformas, aplicaciones y servicios incluyen patrones adictivos para aumentar su tiempo de conexión. Esta presentación ha tenido lugar durante el curso [Nuevos retos para la protección de los derechos de las personas ante el impacto de Internet](#), enmarcado en las Actividades de Verano 2024 de la Universidad Internacional Menéndez Pelayo (UIMP) de Santander.

El informe pone de manifiesto cómo, en muchos casos, estos proveedores implementan patrones de diseño engañosos y adictivos para prolongar el tiempo que los usuarios permanecen en sus servicios o para incrementar su nivel de compromiso y la cantidad de datos personales que se recogen sobre ellos. El impacto adverso de las estrategias adictivas es considerablemente mayor cuando se utilizan para tratar datos personales de personas vulnerables, como es el caso de la infancia y adolescencia, **influyendo en las preferencias e intereses de los menores y afectando en última instancia a su autonomía y a su derecho al desarrollo.**

El Comité Europeo de Protección de Datos (CEPD) abordó los patrones engañosos las [Directrices 03/2022 sobre patrones de diseño engañosos en interfaces de plataformas de redes sociales: cómo reconocerlos y evitarlos](#). La Agencia ha realizado en el informe una revisión de la evidencia científica existente acerca de los patrones adictivos en diferentes plataformas, aplicaciones y servicios (redes sociales, pero también plataformas de vídeo o música, de contenido para adultos, juegos, entornos de aprendizaje, aplicaciones de salud y bienestar, etc.) lo que supone abordar, desde una perspectiva complementaria, nuevos casos de uso.

Por otra parte, el Reglamento de Servicios Digitales, conocido como Digital Services Act (DSA) establece en su artículo 25 que las plataformas online no diseñarán, organizarán ni gestionarán sus interfaces de manera que engañen o manipulen a los usuarios, o de manera que distorsionen u obstaculicen su capacidad de tomar decisiones libres e informadas.

Puede ver más información en el siguiente enlace:

[Patrones adictivos en el tratamiento de datos personales](#)

## EL PROFESIONAL RESPONDE

### ¿Cómo puedo proteger de los ciberataques los activos principales de mi empresa?

Existen muchos tipos de virus y según su comportamiento y modo de acción se les denomina de una forma u otra. Algunos virus pueden atacar directamente mientras que otros buscan solamente activarse y reproducirse, en cualquier caso, todos ellos pretenden causar daño y obtener un beneficio económico.

En este artículo y siguientes vamos a analizar algunos de los virus y *malware* principales que podemos encontrar y cómo protegernos:

**Adware:** es un tipo de *software* que muestra publicidad no deseada o engañosa. Estos anuncios pueden aparecer en nuestro navegador mediante ventanas emergentes (con la finalidad de generar ingresos para sus creadores. Puede ocurrir, que este *software* cambie el motor de búsqueda predeterminada por el usuario y provocar errores en las búsquedas y dificulta la navegación. **¿Cómo podemos protegernos?** Entre otras medidas, debemos evitar abrir enlaces de descarga de sitios poco fiables, y en el caso de necesitar instalar un *software* revisar los pasos para asegurarnos de que no se instalan otros programas o complementos sin darnos cuenta. Actualizar el software regularmente, configurar el navegador ajustando la configuración de seguridad y privacidad para minimizar el riesgo. Utilizar herramientas *anti-malware* para escanear el dispositivo.



#### IMPORTANTE

La formación en ciberseguridad es crucial para protegerse contra amenazas digitales y mantener la información de la empresa segura.