



JORNADA
**APLICANDO LA
NUEVA
NORMATIVA
SOBRE
PROTECCIÓN
DE DATOS**

VALLADOLID, 17 DE OCTUBRE 2018

ACERCÁNDONOS A LOS CONCEPTOS BÁSICOS EN PROTECCIÓN DE DATOS

Fernando Bigeriego Tejerina
Jefe de Área de Atención al Ciudadano
AEPD





Acercándonos a los conceptos básicos en protección de datos

Fernando Bigeriego

*Jefe de área de
Atención al Ciudadano*



- 1. El derecho fundamental a la protección de datos personales. Diferencias con el derecho a la intimidad.**
- 2. Normativa de aplicación y ámbito de aplicación.**
- 3. Conceptos básicos.**
- 4. Principios del tratamiento.**



El derecho fundamental a la protección de datos personales. Diferencias con el derecho a la intimidad.



- **Constitución Española:** artículo **18.4**: *“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.
- Jurisprudencia TC:
 - **STC 94/1998:** Derecho fundamental autónomo e independiente del derecho fundamental al honor, intimidad personal y familiar y propia imagen.
 - **STC 292/2000:** “Autodeterminación informativa”: poder de disposición y de control sobre los datos personales:
 - Faculta para decidir cuáles de esos datos proporcionar a un tercero.
 - Permite saber quién posee esos datos y para qué, pudiendo oponerse a ello.



- **Contexto:** sociedad del conocimiento (“limitación del uso de la informática”).
 - Información como principal vector de crecimiento económico.
 - Datos como input esencial para la creación de valor.
 - Incremento del volumen de datos y de la capacidad para tratarlos.
 - Manifestaciones: redes sociales, apps, motores de búsqueda, economía colaborativa, Big Data, Internet de las cosas...



- **“Teoría del mosaico”**: cualquier dato es relevante.
- **Riesgos**:
 - Creación de perfiles que determinan el acceso o no del individuo a bienes y servicios: empleo, créditos, vivienda, seguros...
 - Publicidad comportamental.
 - Falta de olvido: “la muerte de la amnesia”.
 - Descontextualización de la información.
 - Mermas económicas.



El sistema de valoración social de Black Mirror llega a China

JESÚS ROMERO 22.03.2018 - 14:49H



- El sistema Zhima Credit monitoriza cada paso de la vida de los ciudadanos chinos.
- Sus perfiles determinarán una puntuación que les permitirá acceder o no a ciertas cosas.



Escena del capítulo 'Nosedive', de la tercera temporada de 'Black Mirror'. NETFLIX

Parece que Black Mirror no se equivocaba... el control de la sociedad en todos sus ámbitos se ha hecho realidad, **el horror jerárquico ha llegado a China**. Hace unos meses, el gobierno chino planteaba un sistema de valoración social que ahora se ha tornado como real para los ciudadanos asiáticos. Desde este momento, todos los movimientos financieros, las compras, las opiniones sobre política o incluso, los comportamientos cívicos serán monitorizados y sometidos a las puntuaciones del sistema **Zhima Credit**. Este método elaborará un perfil de

BLOGS DE 20MINUTOS



VEINTE SEGUNDOS

Sánchez e Iglesias firman el Pacto del Pilar y se van de puente... pero ¿dónde están los 900 euros?



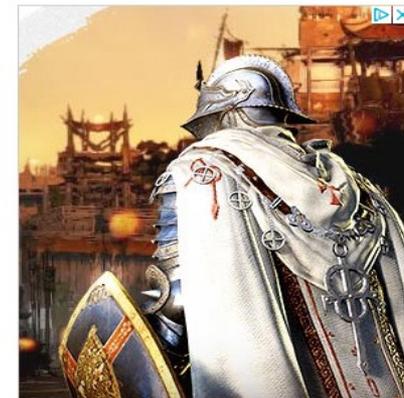
LA ENERGÍA COMO DERECHO

La energía como derecho



¿QUÉ FUE DE?

Camisetas para la historia. Segunda equipación de Francia 2011/2012: el estilo marinero





- **STC 254/1993:** el artículo 18.4 de la Constitución consagra un **derecho fundamental autónomo y diferente** del derecho a la intimidad: *“una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas: el uso ilegítimo del tratamiento mecanizado de datos”*.
- **Distinta función:**
 - Protección de datos: garantizar control de los datos personales.
 - Intimidad: proteger frente a invasiones en la vida privada o familiar.
- **Distinto objeto:**
 - Protección de datos: cualquier tipo de datos.
 - Intimidad: datos íntimos.
- **Distinto contenido:**
 - Protección de datos: obligaciones e instrumentos para hacerlo efectivo: derechos frente al responsable.
 - Intimidad: no.
- **Derecho instrumental.**



Normativa de aplicación y ámbito de aplicación.



- **Declaración Universal de Derechos Humanos:** artículos **12 y 19:** principio de protección de los ciudadanos frente a la intromisión en su vida privada y derecho a la libertad de opinión y de expresión.
- **Convenio nº 108 del Consejo de Europa** de 1981, ratificado por España en 27 de enero de 1984, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.



- **Constitución Española:** artículo **18.4**: *“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*.
- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO** de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (**RPGD**)
- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.



En todo lo que no se oponga al RGPD, seguirá siendo de aplicación, hasta la aprobación del Proyecto de Ley Orgánica de Protección de Datos:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**LOPD**).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (**RLOPD**).
- Instrucciones de la AEPD.



- Directiva 2016/680, de 27 de abril de 2016, del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (**LGT**).
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (**LSSI**).



El RGPD se aplica:

- Al tratamiento total o parcialmente automatizado de datos personales.
- Al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.



Tratamientos excluidos:

- Actividades no comprendidas en el ámbito del Derecho de la UE. Ejemplo: seguridad nacional.
- Actividades comprendidas en el capítulo 2 del Título V del TUE: PESC.
- Efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Ejemplo: agendas personales.
- Ámbito de aplicación de la Directiva 2016/680.
- Datos de personas fallecidas.
- Datos de personas jurídicas.



- Criterio del **establecimiento** en la UE: actividades de un **establecimiento** del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no.
- Tratamiento de datos personales de interesados que se encuentren en la UE por responsables o encargados **no establecidos** en la UE, en dos casos:
 - Oferta de bienes y servicios: indicios (idioma, moneda, teléfono de contacto).
 - Control de su comportamiento en la UE

Han de nombrar un representante en la UE.



Conceptos básicos.



- **Dato personal:** toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- Ejemplos: nombre y apellidos, imagen, DNI, correo electrónico, dirección IP.
- ¿Nº de móvil? ¿Matrícula?



- **Categorías especiales de datos:** datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.
- **Datos genéticos:** en particular del análisis de una muestra biológica de tal persona. Por ejemplo: ADN.
- **Datos biométricos:** huella dactilar, reconocimiento facial, huella de la oreja, patrón venoso de una mano, forma de caminar de una persona...



- **Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- Padrón municipal de habitantes
- Concesión de subvenciones y ayudas
- Imposición de sanciones
- Otorgamiento de licencias o autorizaciones
- Gestión de tributos
- Registros de documentos
- Gestión de recursos humanos
- Sistema educativo



- **Fichero**: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.
 - Si no: no es fichero.
- **Responsable del tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.
- **Encargado del tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
 - Ejemplos: gestoría laboral o fiscal, contratación de servicios informáticos, servicios de marketing, computación en la nube...
 - NO: personas autorizadas bajo la autoridad del responsable.



- Entre responsable y encargado: **contrato o acto jurídico** que vincule al encargado respecto del responsable y con el contenido del artículo 28 RGPD:
 - Encomiendas de gestión
 - Convenios.
 - Contratos.
 - Norma organizativa: se atribuyen funciones a una unidad transversal.
- Evolución de la figura del encargado en el RGPD: obligaciones y responsabilidades.



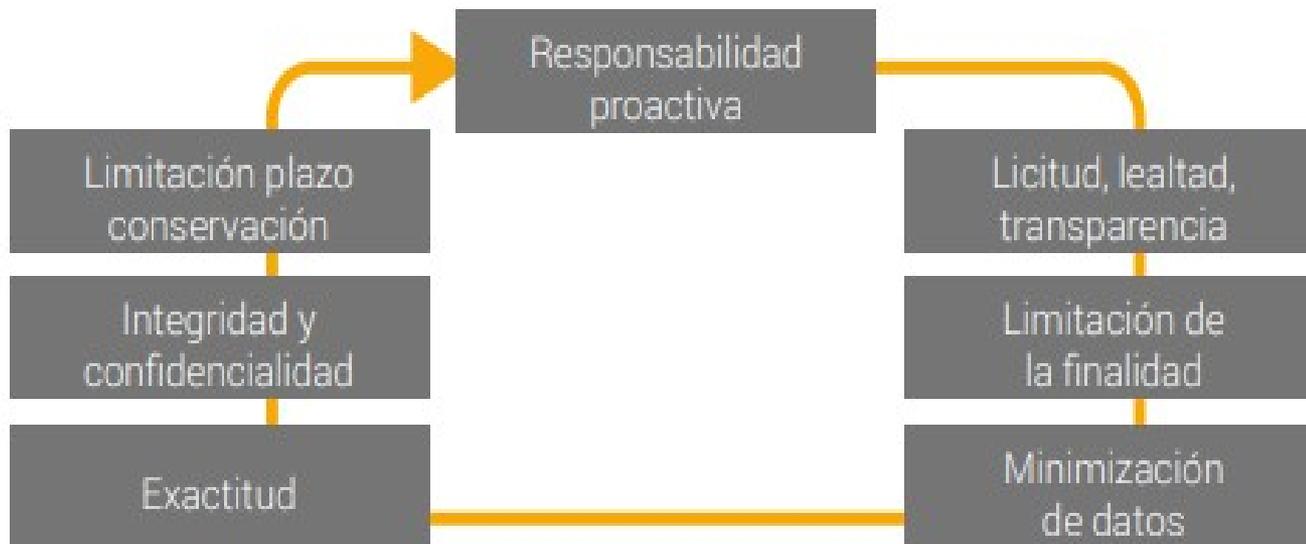
- **Consentimiento:** manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos que le conciernen.
- **Violación de la seguridad de los datos:** la que ocasione la destrucción, 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.
- **Seudonimización:** tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.



- **Elaboración de perfiles:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.
 - Ejemplos: publicidad conductual, perfiles de solvencia, perfiles en base a tecnología Big Data.
- **Bloqueo de datos:** La identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas.



Principios del tratamiento.





- **Licitud**: tratamiento amparado en una base jurídica del RGPD.
- **Lealtad**: no tratamiento desleal o sin información para el interesado.
- **Transparencia**: información que debe proporcionarse al interesado (en qué forma, en qué momentos) y cómo ha de responderse a las solicitudes de ejercicio de derechos.



- **Datos recogidos con fines determinados, explícitos y legítimos:**
 - **Fines determinados:** claramente definidos. Ejemplo: *“Para mejorar su experiencia como usuario”* no sirve.
 - **Fines explícitos:** expresados de forma clara.
 - **Fines legítimos:** permitidos por el ordenamiento jurídico.
- **No tratados ulteriormente de manera incompatible con esos fines.**
 - Compatibilidad de fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.
 - Test de verificación.



- **Test de verificación** (artículo 6.4 del RGPD):
 - Relación entre los fines.
 - Contexto de la recogida de los datos.
 - Naturaleza de los datos: categorías especiales o no.
 - Consecuencias para los interesados.
 - Garantías adecuadas: cifrado, seudonimización.



- **Adecuados:** aportan información relacionada con la finalidad.
- **Pertinentes:** no lo será si puede prescindirse de él.
- **Limitados a lo necesario:** matiz respecto a la Directiva, que hablaba de datos “no excesivos”.

Considerando 39: *“Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios”.*



- **Exactos y actualizados**
 - Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos inexactos
 - Como consecuencia del derecho de rectificación o por iniciativa del responsable.



- Manifestación temporal del principio de minimización: conservarse durante no más tiempo del necesario para alcanzar los fines.
- Después: borrados o anonimizados.
- Excepciones:
 - Conservación para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos
 - Conservación por obligación legal del responsable.



- Novedad del RGPD.
- **Integridad**: medidas que garanticen la inalterabilidad de los datos almacenados.
- **Confidencialidad**: medidas que impidan accesos no autorizados: “need to know” o “necesidad de saber”.



- Doble lectura:
 - **El responsable del tratamiento** es responsable del cumplimiento del RGPD, por ser quien decide los fines y medios.
 - **Novedad del RGPD: No es suficiente con no incumplir:** se exige proactividad, adopción de medidas preventivas y capacidad de demostrarlo (“accountability”, “rendición de cuentas”). Es esencial la **trazabilidad**, documentar todas las decisiones.

A G E N C I A
E S P A Ñ O L A D E
P R O T E C C I Ó N
D E D A T O S



www.aepd.es

[@AEPD_es](https://twitter.com/AEPD_es)