GUÍA LEGAL BÁSICA DE LA PRIVACIDAD

Roberto L. Ferrer Serrano

ABOGADO

aralegis

LOS ÁMBITOS DE NUESTRA VIDA EN SOCIEDAD

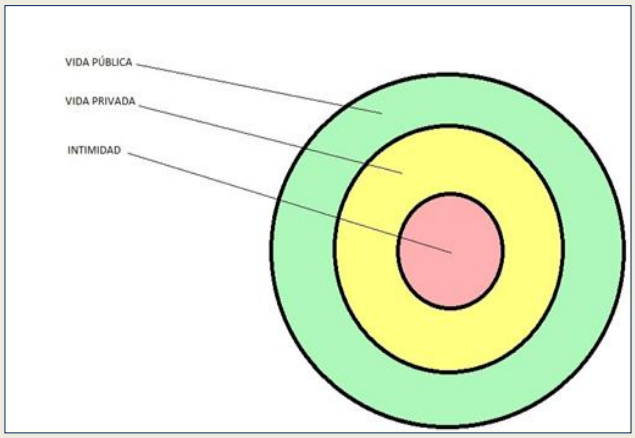
Para poder entender toda la construcción legal creada en torno a la protección de datos de carácter personal necesitamos conocer primero cuales son los ámbitos en los que las personas nos movemos dentro de la sociedad. En nuestra vida en sociedad tenemos tres ámbitos diferentes:

LO PÚBLICO que es la parte de nuestra vida que no puede ocultarse por ser visto o sabido por cualquier otra persona. La **publicidad** es *la cualidad o estado de algo que es público.*

LO PRIVADO que incluye cualquier aspecto de la vida que sea personal y particular de cada individuo. La **privacidad** es el *ámbito de la vida, privada que se tiene derecho a proteger de cualquier intromisión.*

LO ÍNTIMO que se corresponde con la parte más interior o interna de la persona. La **intimidad** es *aquella zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*

Este tipo de definiciones se ha visto explicado por la llamada **TEORÍA DE LOS CÍRCULOS CONCÉNTRICOS** mediante la cual se simboliza nuestra vida pública en un gran círculo exterior, dentro del cual se encuentra un circulo más pequeño que se corresponde con nuestra vida privada y en el que, a su vez, se incluye un circulo, todavía menor que simboliza nuestra parte más interior.



Sin embargo esta definición hoy ya no resulta suficiente, por eso tiene que complementarse con la llamada **TEORÍA DEL MOSAICO** ya que no basta atender únicamente al tipo de datos exigidos; lo decisivo es su utilidad y la posibilidad de emplearlos. Esto depende, de una parte, de la finalidad a la que sirve su recolección, y de la otra, de las posibilidades de procesamiento y vinculación propias de la tecnología de la información. De ese modo, un dato que por sí mismo puede ser visto como no relevante puede adquirir valor por lo que podemos decir que deja de haber datos "no relevantes".

El perfil personal puede configurarse tesela a tesela, incluso aunque falte algún fragmento (Mosaico Telesado Museo de Zaragoza S III-IV dC. Casa del Juicio de Paris. Foto: Roberto L. Ferrer Serrano)

OBJETO DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Así vemos que la función del **derecho fundamental a la *intimidad*** (artículo 18 CE) *es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, es decir, el poder de resguardar su vida privada de una publicidad no querida.*

En cambio, ***el derecho fundamental a la protección de datos*** *persigue garantizar a esa persona un* ***poder de control*** *sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.*

El objeto del derecho a la protección de datos es **más amplio que el del derecho a la intimidad**, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en

su dimensión constitucionalmente protegida por el art. 18.1 C.E., sino a otros derechos de la personalidad que pertenecen al ámbito de la vida privada, unidos al respeto de la dignidad personal tales como el derecho al honor y al pleno ejercicio de los derechos de la persona.

Como afirma la importante **sentencia del Tribunal Constitucional 292/2000 de 30 de Noviembre**, de este modo, el objeto de protección del derecho fundamental a la protección de datos tiene una doble peculiaridad:

- ✓ De una parte no se reduce sólo a los datos íntimos de la persona, sino a **cualquier tipo de dato personal, sea o no íntimo.**
- ✓ Pero también, dicha peculiaridad radica en su contenido, ya que el derecho a la protección de datos **atribuye a su titular un poder de control sobre sus datos personales**, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.

  A saber:

a) DERECHO DE ACCESO.
b) DERECHO DE SUPRESIÓN.
c) DERECHO DE OPOSICIÓN.
d) DERECHO DE RECTIFICACIÓN.
e) DERECHO DE LIMITACIÓN.
f) DERECHO DE PORTABILIDAD.

¿COMO SE PROTEGE CONSTITUCIONALMENTE EL DERECHO A LA PRIVACIDAD?

El derecho fundamental a la protección de la privacidad, más conocido como derecho de protección de datos, no existe como tal en nuestra Constitución de 1978 y no será hasta el año 2000 cuando se desarrolle por el Tribunal Constitucional (Sentencia 292/2000 de 30 de noviembre) el concepto de derecho fundamental a la protección de datos de carácter personal. Se trata pues de una construcción jurisprudencial y no vinculada a una norma jurídica concreta.

Nuestro Tribunal Constitucional hace derivar de estos poderes de disposición y control sobre los datos personales, una serie de facultades que consisten en consentir:

- *La recogida, la obtención y el acceso a los datos personales.*
- *Su posterior almacenamiento y tratamiento.*
- *Su uso o usos posibles, por un tercero, sea el Estado o un particular.*

De este derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, surgen como complementos indispensables:

- La facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y
- El poder oponerse a esa posesión y usos.

SITUACION ACTUAL DE LA PRIVACIDAD. LA VIDA EN UN MUNDO DE CRISTAL.

Los resultados de las encuestas que podemos estudiar, tanto en España como en la Unión Europea, revelan que **los ciudadanos estamos preocupados por nuestra privacidad pero no**

queremos renunciar a las ventajas que nos reporta la tecnología. Es por ello que tenemos que aprender a conjugar su uso con los inconvenientes o la servidumbre que esto conlleva sabiendo que la moneda de cambio es información sobre nosotros mismos.

En un mundo en el que el progreso parece depender de como se aprovecha la información que todos nosotros vamos generando surge la pregunta de si tendremos que aprender a vivir en un mundo de cristal, como será este de transparente, hasta qué punto podremos limitar que los demás puedan mirar dentro de nuestras vidas y sobre todo deberemos calcular si dentro de un tiempo merecerá la pena vivir en un mundo así.

PRINCIPIOS DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

La normativa sobre protección de datos de carácter personal descansa sobre una serie de pilares fundamentales, sobre los que descansan todos los demás criterios que puedan ser de aplicación. Por ello, si tenemos bien presente que debemos y podemos exigir que el tratamiento de nuestros datos personales respete dichos principios, limitaremos enormemente cualquier abuso.

Principio de finalidad legítima

"Los datos de carácter personal objeto de tratamiento ***no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos****"*

Hay que señalar que la jurisprudencia, además, ha matizado que la expresión *"incompatibles"* en este contexto se refiere a que no se trate de una finalidad distinta a la que motivó el tratamiento de los datos lo que supone una clara reducción de la potestad de utilización de los datos personales por parte de los responsables de los ficheros.

Principio de información

Permite a los ciudadanos conocer de antemano no solamente **la finalidad** para la que se solicitan sus datos, sino todas las **cuestiones que vayan a resultar necesarias para otorgar o no el consentimiento** para que se traten sus datos personales.

A raíz del nuevo *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* (Reglamento 2016/679) la información que deberá facilitarse a los interesados podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

El artículo 13 del Reglamento sí que genera, a diferencia de la normativa anterior, una situación con diferencias relevantes especialmente **para los responsables de los tratamientos que ven ahora incrementada su carga burocrática** habida cuenta de que **los extremos sobre los que sea de informar a los interesados se amplían sustancialmente y de forma mucho más detallada** y ello tanto si esos datos personales se han obtenido del interesado, como cuando no sean obtenidos directamente del mismo.

Principio de consentimiento

Este principio establece una serie **de límites a la utilización de datos personales marcados por la voluntad del ciudadano** que permitirá o no que su identidad u otras circunstancias personales queden almacenadas en ficheros de quienes les suministran algún producto o servicio.

El ámbito de la edad para la prestación del consentimiento del niño en relación con los servicios de la sociedad de la información en el Reglamento 2016/679 se encuentra en el artículo 8, en él se eleva con respecto a la regulación española la edad mínima a 16 años, en lugar de los 14 que establece nuestra regulación si bien se contempla la posibilidad de que los Estados miembros puedan establecer por ley una edad inferior siempre que ésta no sea inferior a 13 años. Ello significa que nuestro Reglamento carece de habilitación legal para fijar una edad inferior a los 16 años (se necesitaría una Ley).

Principio de exactitud y principio de veracidad

El artículo 5,1d) establece que los datos personales serán "d*) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)*".

Principio de garantía

Afecta al tratamiento de los datos personales por las personas y entidades que participan del mismo.

Principio de responsabilidad

Las organizaciones tendrán que implementar medidas que permitan acreditar que están adoptando todas las medidas necesarias para realizar un **correcto tratamiento de los datos personales.**

El **considerando 146 del Reglamento 2016/679** nos dice que:

• El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del Reglamento. Su responsabilidad es solidaria.

• El concepto de daños y perjuicios debe interpretarse en sentido amplio. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos.

• La responsabilidad se derivará no solamente al responsable del tratamiento sino también a la entidad en la que se puedan externalizar los tratamientos de datos, ampliándose el alcance la Directiva.

• Se amplía el concepto de daño y se extiende más allá de la perdida financiera.

• Las empresas tendrán que establecer cláusulas contractuales claras y garantías para protegerse de responsabilidad.

Principio de protección de datos por defecto y desde el diseño

Las organizaciones tendrán que implementar medidas que permitan **acreditar que están adoptando todas las medidas necesarias para**

realizar un correcto tratamiento de los datos personales.

• Éste es uno de los nuevos conceptos llamados a jugar un papel central, **seudonimizando** los datos siempre que sea posible.

• Deberá tenerse en cuenta cuando dicha seudonimización sea **reversible**.

• Las empresas **no deberán tratar datos a menos que pueda justificarse una finalidad legítima** y se haya documentado el impacto sobre la privacidad y como estarán seguros los datos mediante políticas que deberán estar actualizadas.

• Orientados a adoptar la **cultura de la privacidad** en el seno de la organización y **garantizar la privacidad** de las personas.

• **La privacidad se incorpora al proceso productivo** desde el diseño de cualquier producto o servicio.

• Los productos o servicios deben configurarse inicialmente con los mecanismos más amplios de privacidad.

Principio de responsabilidad y registro (ACCOUNTABILITY).

• **Simplificación de los avisos legales y clausulados** facilitando su comprensión por las personas cuyos datos van a ser tratados.

• Aplicable tanto a los responsables de tratamiento como a los encargados de tratamiento. Ellos deberán mantener **registros del cumplimiento de sus obligaciones.**

Otras acciones a adoptar por los responsables del tratamiento son:

• Auditar los datos personales tratados por la entidad comprobando

• Qué datos personales se procesan

• La razón de su procesamiento

• Cómo se están usando

• Donde se mantienen comprobando si es necesario mantenerlos y

• Si se utilizan con finalidades diferentes a las que se recabaron.

Principio de gratuidad

Excepción: Cuando las **solicitudes sean manifiestamente infundadas o excesivas**, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento deberá demostrar el carácter manifiestamente infundado o excesivo de una solicitud para denegarla.

OTRAS OBLIGACIONES DE LOS RESPONSABLES DE LOS TRATAMIENTOS DE DATOS PERSONALES

La notificación de brechas de seguridad de los datos. Artículo 33 del RGPD.

Roberto L. Ferrer Serrano

El responsable del tratamiento deberá **notificar una violación de datos personales a la autoridad de supervisión competente dentro de las 72 horas** siguientes a tener conocimiento de esta. **Excepciones:**

• Cuando la violación de datos es *"poco probable que resulte riesgo para los derechos y libertades de las personas físicas"*

• Si es *"probable que resulte en un alto riesgo para los derechos y libertades de las personas físicas"* el responsable del tratamiento debe notificarle esta al interesado *"en tiempo oportuno"* incluso en menos de 72 horas.

Acciones a adoptar por las Entidades.

En el caso de una violación de seguridad, habrá muy poco tiempo para determinar la magnitud de los daños, los individuos afectados, las medidas de seguridad que tienen que ser modificadas o reforzadas, y determinar si la situación requiere la notificación a la autoridad nacional de protección de datos y/o a las personas interesadas.

Por ello se deberán:

• Establecer **procedimientos de violación de la seguridad cibernética.**

• Establecer **procedimientos de contingencia** para tomar tales decisiones, y las personas que se encargarán de hacerlas.

• Deberá haber coordinación con los responsables de comunicación para minimizar daños reputacionales.

Designación de un Delegado de Protección de Datos (DPO).

Esta medida se adoptará siempre que:

a) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Acciones a adoptar por las entidades: Las empresas deben evaluar con antelación si van a estar obligados a designar un DPO antes del 25 de Mayo de 2018.

El régimen de extraterritorialidad y alcance.

El nuevo régimen **se aplica tanto a controladores como a procesadores de datos** de cualquier parte del mundo* que, o bien:

a) Ofrecen bienes o servicios a los interesados en la UE (sean o no de pago)

b) Monitorizan el comportamiento de los individuos dentro de la UE.

*Se incluye cualquier lugar donde sea aplicable la ley de un Estado miembro de la UE en virtud del derecho internacional público (Por ejemplo en el interior de las embajadas o a bordo de buques o aeronaves registradas en un Estado miembro de la UE.)

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

Una transferencia internacional de datos es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

Tipos de transferencias de datos personales:

Transferencias basadas en una decisión de adecuación (Artículo 45 Reglamento 2016/679).

Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando **la Comisión haya decidido** que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate **garantizan un nivel de protección adecuado.** Dicha transferencia no requerirá ninguna autorización específica.

Roberto L. Ferrer Serrano

Transferencias mediante garantías adecuadas (Artículo 46 Reglamento 2016/679).

A falta de decisión con arreglo al artículo anterior, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido **garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.**

Normas corporativas vinculantes (Artículo 47 Reglamento 2016/679).

La autoridad de control competente aprobará **normas corporativas vinculantes de conformidad con el mecanismo de coherencia** establecido en el artículo 63 del Reglamento 2016/679.

Excepciones para situaciones específicas (Artículo 49 Reglamento 2016/679).

En ausencia de una decisión de adecuación, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones del art. 49.

Privacy Shield Framework

La Comisión Europea aprobó formalmente la adecuación del acuerdo **"escudo de privacidad"** el día 12 de Julio de 2016 aceptándose autocertificaciones de empresas estadounidenses a partir del 1 de Agosto de 2016 de forma similar al sistema anterior debiendo verificarse 7 principios de privacidad de forma más exigente especialmente en lo relativo a la verificación de su cumplimiento y el establecimiento de compensaciones en caso de infracción a dichos principios[1].

[1]Más información sobre el esquema se puede encontrar

¿QUÉ RIESGOS TIENE INCUMPLIR LA NORMATIVA DE PROTECCIÓN DE DATOS?

Una de las cuestiones más conocidas y que más llaman la atención es la importancia de las sanciones que el incumplimiento de la normativa de protección de datos puede conllevar.

Infracciones y sanciones

El **sistema de control** del cumplimiento de la normativa de protección de datos de *carácter personal se fundamenta en* ***la imposición de una*** **serie de sanciones**. Según el artículo 83 del RGPD cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo a dicho artículo por las infracciones del Reglamento indicadas en los apartados 4, 5 y 6 del art. 83 sean en cada caso individual **efectivas, proporcionadas y disuasorias.**

En cuanto a las sanciones a imponer

En virtud del artículo 83, las autoridades nacionales de supervisión tendrán la facultad de imponer multas:

Graves: hasta 10 millones de €, o el 2% del total volumen de negocios mundial de una empresa en el ejercicio anterior (la mayor de las 2 opciones).

Muy Graves: hasta 20 millones de €, o el 4% del total volumen de negocios mundial de una empresa en el ejercicio anterior (la mayor de las 2 opciones).

Los Estados miembros también deben establecer normas sobre otras sanciones aplicables a las infracciones del Reglamento, y deben tomar *"todas las medidas necesarias para garantizar que su aplicación ... dichas sanciones deberán ser efectivas, proporcionadas y disuasorias."* La definición concreta de cada tipo de infracción se establece en el mismo artículo conforme a la siguiente tabla:

INFRACCIONES EN LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS

Graves: Multa de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4.

Muy graves: Multa de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;
b) los derechos de los interesados a tenor de los artículos 12 a 22;
c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;
d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;
e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

---

en su página web oficial (https://www.privacyshield.gov/welcome)

COMPETENCIA SANCIONADORA

Según el artículo 84 del RGPD los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias. Además cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

Por tanto cada Estado establecerá las correspondientes tipificaciones que deberán encontrarse dentro del marco establecido por la norma europea.

Con arreglo a la normativa española, vigente en la actualidad existen dos regímenes diferenciados:

- Tratamientos de datos de titularidad privada
- Tratamientos de datos de titularidad pública

La diferencia se encuentra en las sanciones a imponer así como en el procedimiento, ya que en cualquiera de los dos regímenes las actuaciones consideradas infractoras son comunes a ambos.

Las conductas infractoras se establecen en el artículo **44 de la Ley Orgánica de Protección de Datos de carácter personal** (L.O. 15/99 de 13 de Diciembre) y se definen como:

- Leves,
- Graves
- Muy graves.

En cuanto a las sanciones a imponer

En el caso de Tratamientos de datos de titularidad privada se aplica el artículo 45, 1 al 3 que establece:

1. Las **infracciones leves** serán sancionadas con multa de 900 a 40.000 euros.
2. Las **infracciones graves** serán sancionadas con multa de 40.001 a 300.000 euros.
3. Las **infracciones muy graves** serán sancionadas con multa de 300.001 a 600.000 euros.

La definición concreta de cada tipo de infracción se establece en el mismo artículo conforme a:

INFRACCIONES A LA NORMATIVA NACIONAL DE PROTECCIÓN DE DATOS

Leves: Multa de 900 a 40.000 euros.

a) **No remitir a la Agencia Española de Protección de Datos las notificaciones previstas** en esta Ley o en sus disposiciones de desarrollo.

b) **No solicitar la inscripción del fichero** de datos de carácter personal **en el Registro General de Protección de Datos.**

c) El **incumplimiento del deber de información al afectado** acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

d) **La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales** establecidos en el artículo 12 de esta Ley.

Graves: Multa de 40.001 a 300.000 euros.

a) **Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos**

de carácter personal para los mismos, s**in autorización de disposición general**, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

b) **Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas**, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.

c) **Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías** establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.

d) **La vulneración del deber de guardar secreto** acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.

e) **El impedimento o la obstaculización del ejercicio de los derechos** de acceso, rectificación, cancelación y oposición.

f) **El incumplimiento del deber de información al afectado** acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

g) **El incumplimiento de los restantes deberes de notificación o requerimiento al** afectado impuestos por esta Ley y sus disposiciones de desarrollo.

h) **Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal** sin las debidas condiciones de seguridad que por vía reglamentaria se determinen

i) **No atender los requerimientos o apercibimientos de la Agencia** Española de Protección de Datos **o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados** por la misma.

j) La **obstrucción al ejercicio de la función inspectora**.

k) **La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello** en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

Muy graves: Multa de 300.001 a 600.000 euros.

a) La **recogida de datos en forma engañosa o fraudulenta**.

b) **Tratar o ceder los datos de carácter personal a los** que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.

c) **No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia** Española de Protección de Datos para ello.

d) **La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia** Española de Protección de Datos salvo en

aralegis

los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

CRITERIOS DE GRADUACIÓN DE LAS SANCIONES

Sin embargo dada la amplitud de la escala sancionadora, el punto 4 del mismo artículo establece para la **graduación de la sanción los siguientes criterios:**

- **a)** El carácter continuado de la infracción.
- **b)** El volumen de los tratamientos efectuados.
- **c)** La vinculación de la actividad del infractor con la realización de tratamientos de datos.
- **d)** El volumen de negocio o actividad del infractor.
- **e)** Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- **f)** El grado de intencionalidad.
- **g)** La reincidencia por comisión de infracciones de la misma naturaleza.
- **h)** La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
- **i)** La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
- **j)** Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Un elemento muy importante a tener en cuenta es **la posibilidad de reducir la graduación de la infracción a la escala anterior**, lo puede resultar fundamental en muchos supuestos ya que una infracción que se castigaría con 300001 euros puede reducirse a 900 euros en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente

APERCIBIMIENTO

Otra posibilidad que puede aplicarse es **el apercibimiento** que se considera una posibilidad excepcional en la que el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios

establecidos para reducir las sanciones a la escala precedente (antes indicados), podrá no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes.

Para que exista esta posibilidad **han de concurrir los siguientes presupuestos:**

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento

En el caso de tratamientos de titularidad pública se aplica el artículo 46 que establece:

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

LA INMOVILIZACIÓN DE FICHEROS

Como medida excepcional se encuentra prevista una medida adicional consistente en la inmovilización de ficheros

Artículo 49. Potestad de inmovilización de ficheros.

En los **supuestos constitutivos de infracción grave o muy grave** en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y en particular de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido,

el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

LA PRESCRIPCIÓN DE LAS INFRACCIONES Y SANCIONES

La prescripción de las infracciones y sanciones finalmente se encuentra regulada en el artículo 47 de la vigente Ley Orgánica de Protección de Datos de carácter personal (L.O. 15/99 de 13 de Diciembre)

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Roberto L. Ferrer Serrano

ALGUNOS CONCEPTOS ÚTILES

1) **«datos personales»:** toda **información sobre una persona física identificada o identificable** («el interesado»); 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;

2) **«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;

3) **«grupo empresarial»:** grupo constituido por una **empresa que ejerce el control y sus empresas controladas**;

4) **«representante»: persona física o jurídica establecida en la Unión que**, **habiendo sido**

designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, **represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones** en virtud del presente Reglamento;

5) **«seudonimización»:** el **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;

6) **«fichero»:** todo **conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica**;

7) **«responsable del tratamiento» o «responsable»:** la **persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento;** si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) **«encargado del tratamiento» o «encargado»**: la **persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento**;

9) **«destinatario»:** la **persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero**. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) **«tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas** para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

aralegis

Normativa básica

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**.**

Ley Orgánica de Protección de Datos de carácter personal, 15/99 de 13 de Diciembre.

Real Decreto 1720/2007 Reglamento de la Ley Orgánica de Protección de Datos de carácter personal

Ley 34/2002, de 11 de Julio de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Ley General de Telecomunicaciones, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Ley 16/2006, de 28 de diciembre, de Protección y Defensa de los Ciudadanos y Usuarios de Aragón.

Ley 26/1984, de 19 de julio, General para la Defensa de los Ciudadanos y Usuarios.