

# El tratamiento de la información y el informe no financiero de las sociedades de capital: una inclusión necesaria

Revista de Derecho vLex - Núm. 237, Febrero 2024

**Autor:** Alberto Palomar Olmeda

**Cargo:** Abogado, Profesor Titular de Derecho Administrativo (a) y Magistrado (ev)

**Id. vLex:** VLEX-999022761

**Link:** <https://app.vlex.com/vid/tratamiento-informacion-informe-no-999022761>

## Resumen

La tesis fundamental del presente trabajo es la necesidad de incluir en el marco de los informes no financieros de las sociedades mercantiles el conjunto de riesgos que proceden del tratamiento y, en consecuencia, de las técnicas de destrucción de la misma como garantía del adecuado tratamiento y como elemento vinculado a la privacidad de las personas y a las garantías de los derechos fundamentales que, según la regulación específica, forman parte ineludible de la reflexión de la respectiva organización.

## Texto

# Contenidos

- [La gobernanza institucional de las organizaciones.](#)
- [Algunos instrumentos de objetivación de los criterios y las formas del buen gobierno.](#)
  - [El contexto europeo.](#)
  - [Regulación española.](#)
    - [Cuentas anuales.](#)
    - [Cuentas anuales consolidadas.](#)
    - [Comisión Europea.](#)
- [Tratamiento de la información y los riesgos de afección a los derechos fundamentales.](#)
- [Algunas referencias a la destrucción de la información como elemento de preservación de valores diversos legalmente asumidos.](#)
  - [Normativa administrativa.](#)
  - [Ejemplos de leyes de ámbito general que se proyectan sobre el régimen jurídico de](#)

### la conservación documental.

- [Ley General Tributaria.](#)
- [Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica.](#)
- [Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad del Estado en lugares públicos.](#)
- [Ley de Seguridad Aérea.](#)
- [Las políticas de borrado y destrucción de la información como parte de la garantía de la correcta utilización y del cumplimiento de las obligaciones en dicho ámbito.](#)

**Abstract.-** La tesis fundamental del presente trabajo es la necesidad de incluir en el marco de los informes no financieros de las sociedades mercantiles el conjunto de riesgos que proceden del tratamiento y, en consecuencia, de las técnicas de destrucción de la misma como garantía del adecuado tratamiento y como elemento vinculado a la privacidad de las personas y a las garantías de los derechos fundamentales que, según la regulación específica, forman parte ineludible de la reflexión de la respectiva organización.

**Abstract.-** The fundamental thesis of this work is the need to include in the framework of the non-financial reports of commercial companies the set of risks that come from the treatment and, consequently, from the destruction techniques of the same as a guarantee of the adequate treatment and as an element linked to the privacy of people and the guarantees of fundamental rights that, according to the specific regulation, form an unavoidable part of the reflection of the respective organization.

**Palabras clave:** informe no financiero, auditoría de cuentas, tratamiento de la información, técnicas de borrado, privacidad, derechos de las personas.

**Keywords:** non-financial report, account audit, information processing, erasure techniques, privacy, people's rights.

## La gobernanza institucional de las organizaciones

No es fácil señalar cuál es el momento y, probablemente, tampoco la causa única, por la que el Derecho mercantil y, específicamente, el Derecho de sociedades, comienza a darse cuenta de que el **régimen meramente formal** de la **organización interna**, remitida a los estatutos y normas generales, resulta **insuficiente** frente a una sociedad que, en gran medida, asiste atónita a las circunstancias que le ponen ante el brete social de la ineficiencia.

Sea cual sea este momento es lo cierto que hoy podemos indicar que la situación viene de largo y que han sido muchos los intentos de las entidades asociativas de encontrar **fórmulas internas de legitimación de su actuación**, de control y fijación de las competencias y procedimientos para asegurar una correcta toma de decisiones a favor de los accionistas y de las personas que

se relacionan con la sociedad. En esta labor las entidades han estado vinculadas a las organizaciones empresariales y de disciplina social en relación con estos requisitos.

En esencia, el planteamiento es sencillo: la **regularidad procedimental** contribuye a la legitimación social de las empresas, a la rectitud como criterio de su presencia y su actuación social y, finalmente, a la seguridad de la correcta actuación frente a la propia organización y los externos que se relacionan con la misma.

A este esquema de cumplimiento interno, de **auto regulación**, de disciplina organizativa se le ha denominado como “buena gobernanza” o “buen gobierno”, expresiones que, realmente, lo que reflejan es que la organización es capaz de ordenar su vida interna y, sobre todo, de cumplir el esquema que la propia organización considera como su pauta de funcionamiento y organización en función del contexto social y de las propias necesidades. Adicionalmente se ha caracterizado por la diferenciación orgánica de las competencias y el establecimiento de contrapesos en el ámbito de la gestión de forma que se asegure el correcto funcionamiento del sistema.

## Algunos instrumentos de objetivación de los criterios y las formas del buen gobierno

Es cierto que las breves consideraciones que se han hecho en el apartado anterior tienen como característica la **capacidad autoorganizativa y de fijación de los respectivos estándares** de cumplimiento en función de la propia organización y, en función, también de los propios procesos de organización y funcionamiento.

Esta es, sin duda, una de las posibilidades que consiste, precisamente, en dejar el cumplimiento o la buena gobernanza a los estándares que haya fijado la respectiva organización. Pero es cierto que, al lado de esta posibilidad, han ido creciendo otras: nos referimos, fundamentalmente, a los **procesos de estandarización y acreditación de procedimientos o productos** como garantía de una actuación en el marco común de desarrollo de la actividad<sup>1</sup>. La normalización de procedimientos y de productos sobre la base de un estándar es un elemento central del aseguramiento de la propia actividad.

En este sentido, primero, en el tiempo, fue el deseo de presentar ante la sociedad el cumplimiento de los **estándares de calidad** de los productos y de los procesos (que se identifica con las ISO 9000), posteriormente, el respeto ambiental de productos y procesos (que se identifica con las ISO 14.000) y, finalmente, otros elementos que han dado cobertura a reflexiones serenas sobre la posición de las organizaciones.

Este marco de cumplimiento se ha mantenido, a veces, en el plano interno del compromiso individual de las sociedades y, en otros momentos, ha recibido la incorporación a diversos instrumentos previstos en las normas legales. **El proceso de incorporación** es, en cierta medida, un proceso que se caracteriza por la madurez del sistema y por la percepción de que la bondad intrínseca de la medida tiene un valor taumátúrgico que exige su salida de las medidas voluntarias para incluirse en el ámbito de las forzosas o, para ser más exactos, los de

cumplimiento indisponible en función, precisamente, de la posición que el legislador mantiene sobre las mismas.

## El contexto europeo

Tomamos como ejemplo la

[Ley 11/2018, de 28 de diciembre, por la que se modifica el Código de Comercio](#), el texto refundido de la Ley de Sociedades de Capital aprobado por el Real Decreto Legislativo 1/2010, de 2 de julio [\[Ver\]](#), y la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, en materia de información no financiera y diversidad [\[Ver\]](#).

En concreto, la Exposición de Motivos de la propia [Ley 11/2018](#) nos da la pista esencial de su verdadera procedencia cuando señala que «...[La Directiva 2014/95/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2014](#), por la que se modifica la Directiva 2013/34/UE en lo que respecta a la divulgación de información no financiera e información sobre diversidad por parte de determinadas grandes empresas y determinados grupos [\[Ver\]](#), tiene como objetivo **identificar riesgos** para mejorar la sostenibilidad y aumentar la confianza de los inversores, los consumidores y la sociedad en general y para ello incrementa la divulgación de información no financiera, como pueden ser los factores sociales y medioambientales...».

El preámbulo de la [Directiva](#) sitúa a este en el marco de la Comunicación titulada «Acta del Mercado Único — Doce prioridades para estimular el crecimiento y reforzar la confianza — “Juntos por un nuevo crecimiento”», adoptada el 13 de abril de 2011, donde la Comisión Europea señalaba la necesidad de **aumentar la transparencia de la información social y medioambiental** facilitada por las empresas de todos los sectores a un nivel alto similar en todos los Estados miembros<sup>2</sup>.

La importancia de la transparencia en esta materia se plasma también en el preámbulo de la [Directiva](#) cuando explica que «*De hecho, la **divulgación de información no financiera** resulta esencial para la gestión de la transición hacia una economía mundial sostenible que combine la rentabilidad a largo plazo con la justicia social y la protección del medio ambiente. En este contexto, la divulgación de información no financiera contribuye a medir, supervisar y gestionar el rendimiento de las empresas y su impacto en la sociedad. Así pues, el Parlamento Europeo instó a la Comisión a presentar una propuesta legislativa sobre divulgación de información no financiera por parte de las empresas, que permita una gran flexibilidad en la actuación para tener en cuenta la **naturaleza multidimensional de la responsabilidad social de las empresas** (RSE) y la diversidad de políticas de RSE aplicadas por las empresas, teniendo al mismo tiempo un nivel suficiente de comparabilidad que responda a las necesidades de los inversores y otras partes interesadas, así como a la necesidad de ofrecer a los consumidores un acceso sencillo a la información sobre las repercusiones de las empresas en la sociedad...*»

En este contexto la Unión Europea siente la necesidad de dar **coherencia y comparabilidad de la información no financiera divulgada** en la Unión que justifica la norma en cuestión para conseguir un haz de transparencia en lo relativo a las políticas medioambientales, las de personal, los derechos humanos y la lucha contra la corrupción y el soborno<sup>3</sup>.

La [Directiva](#) contempla un denominado estado no financiero ([art. 19 bis](#)), y un estado financiero consolidado ([art. 29 bis](#)). El contexto normativo está representado por el [artículo 9 bis](#) con el siguiente tenor:

“**Estado no financiero 1.** Las **grandes empresas** que sean **entidades de interés público** que, en sus fechas de cierre del balance, superen el criterio de **un número medio de empleados superior a 500** durante el ejercicio, incluirán en el informe de gestión un estado no financiero que contenga información, en la medida en que resulte necesaria para comprender la evolución, los **resultados y la situación de la empresa**, y el **impacto de su actividad**, relativa, como mínimo, a cuestiones medioambientales y sociales, así como relativas al personal, al respeto de los derechos humanos y a la lucha contra la corrupción y el soborno, y que incluya:

a) una breve descripción del **modelo de negocio** de la empresa;

b) una descripción de las **políticas que aplica la empresa** en relación con dichas cuestiones, que incluya los procedimientos de diligencia debida aplicados;

c) los **resultados** de esas políticas;

d) los **principales riesgos** relacionados con esas cuestiones vinculados a las actividades de la empresa, entre ellas, cuando sea pertinente y proporcionado, sus relaciones comerciales, productos o servicios que puedan tener efectos negativos en esos ámbitos, y cómo la empresa gestiona dichos riesgos;

e) indicadores clave de **resultados no financieros**, que sean pertinentes respecto de la actividad empresarial concreta”.

En esencia se trata de enfrentar a las empresas con su propia actuación en aspectos que aparece expresamente identificado como son los sociales o los medioambientales junto con **otros riesgos** que la propia sociedad puede señalar y que son objeto – en ambos casos- de políticas propias de minimización. Evidentemente en este apartado deben incluirse aquellos que pueden proceder de la determinación específica de una **norma sectorial**.

Por su importancia a los efectos de lo que aquí se analiza cabe indicar que el Informe no financiero incluye las **políticas de prevención y de minimización de riesgos** – en la expresión que hemos utilizado- en función de los procesos de actuación de la respectiva empresa.

Las consideraciones anteriores nos sitúan en un marco en el que, claramente, existe **un compromiso directo** en relación con la organización y la transparencia de las sociedades y con el funcionamiento y sus reglas que han definido las mismas.

Se trata de un concepto abierto que realmente integra determinaciones de un conjunto de disposiciones y de regulaciones porque el propio elemento central al que responde no es, no puede ser, unívoco ni único. Realmente se trata de la configuración de un **marco abierto** en el que se van integrando las obligaciones que proceden de las leyes sectoriales que son las que, realmente, valoran la relevancia de determinados valores que se integran en el compromiso que las sociedades y entidades tienen ante la comunidad en general.

# Regulación española

La transposición a la normativa española en lo que se refiere al **informe de actividades no estrictamente económicas** se produce, como hemos indicado, con motivo de la publicación de la [Ley 11/2018, de 28 de diciembre, por la que se modifica el Código de Comercio](#), el texto refundido de la Ley de Sociedades de Capital aprobado por el Real Decreto Legislativo 1/2010, de 2 de julio [[Ver](#)], y la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, en materia de información no financiera y diversidad [[Ver](#)]<sup>4</sup>.

El [artículo 1](#) de la misma contiene una modificación del [Código de Comercio, aprobado por Real Decreto de 22 de agosto de 1855](#). La modificación afecta a los [apartados 1 y 6](#) del [artículo 44](#) en los siguientes términos:

## Cuentas anuales

«**1. Las cuentas anuales consolidadas** comprenderán el balance, la cuenta de pérdidas y ganancias, un estado que refleje los cambios en el patrimonio neto del ejercicio, un estado de flujos de efectivo y la memoria, consolidados. Estos documentos forman una unidad. **A las cuentas anuales consolidadas se unirá el informe de gestión consolidado que incluirá, cuando proceda, el estado de información no financiera.**»»

Conforme a esta consideración existe una **obligación general de formulación de la cuenta de pérdidas y ganancias** que refleja la situación económica de la empresa en cuestión. Sin la consideración de cuentas anuales pero unido a ellas se formula el **informe de gestión** que debe incluir el estado de información no financiera. En esencia se trata de una valoración del comportamiento de gestión de la entidad en cuestión que se integra, esencialmente, por las obligaciones que para el gestor proceden de diferentes ámbitos sectoriales y que responden a la preservación de valores diferenciados en función, precisamente, de las características de lo protegido.

## Cuentas anuales consolidadas

«**6. Las cuentas y el informe de gestión consolidados**, que incluirá, cuando proceda, el estado de información no financiera consolidado, serán firmados por todos los administradores de la sociedad obligada a formularlos, que responderán de la veracidad de los mismos. Si faltara la firma de alguno de ellos, se señalará en los documentos en que falte, con expresa mención de la causa.»<sup>5</sup>. »

Esta última determinación no deja de ser una **especificidad** en relación con la que, anteriormente, hemos indicado en relación con la formulación general de cuentas y de documentación complementaria a dicha regulación.

El **contenido mínimo** de la información no financiera distingue los dos apartados

que acabamos de señalar en su propia configuración. No obstante, esta diferenciación, parece razonable partir de la información o de la composición general y que, por tanto, es aplicable al conjunto de sociedades o entidades. En concreto, se trata de:

- a) Una **breve descripción del modelo de negocio** del grupo, que incluirá su entorno empresarial, su organización y estructura, los mercados en los que opera, sus objetivos y estrategias, y los principales factores y tendencias que pueden afectar a su futura evolución.
- b) Una **descripción de las políticas** que aplica el grupo respecto a dichas cuestiones, que incluirá los procedimientos de diligencia debida aplicados para la identificación, evaluación, prevención y atenuación de riesgos e impactos significativos y de verificación y control, incluyendo qué medidas se han adoptado.
- c) Los **resultados de esas políticas**, debiendo incluir indicadores clave de resultados no financieros pertinentes que permitan el **seguimiento y evaluación de los progresos** y que favorezcan la comparabilidad entre sociedades y sectores, de acuerdo con los marcos nacionales, europeos o internacionales de referencia utilizados para cada materia.
- d) Los **principales riesgos** relacionados con esas cuestiones vinculados a las actividades del grupo, entre ellas, cuando sea pertinente y proporcionado, sus relaciones comerciales, productos o servicios que puedan tener efectos negativos en esos ámbitos, y cómo el grupo gestiona dichos riesgos, explicando los procedimientos utilizados para detectarlos y evaluarlos de acuerdo con los marcos nacionales, europeos o internacionales de referencia para cada materia. Debe incluirse información sobre los **impactos** que se hayan detectado, ofreciendo un desglose de los mismos, en particular sobre los principales riesgos a corto, medio y largo plazo.
- e) Indicadores clave de **resultados no financieros que sean pertinentes respecto a la actividad empresarial concreta**, y que cumplan con los criterios de comparabilidad, materialidad, relevancia y fiabilidad. Con el objetivo de facilitar la comparación de la información, tanto en el tiempo como entre entidades, se utilizarán especialmente **estándares de indicadores clave no financieros** que puedan ser generalmente aplicados y que cumplan con las directrices de la Comisión Europea en esta materia y los estándares de *Global Reporting Initiative*, debiendo mencionar en el informe el marco nacional, europeo o internacional utilizado para cada materia. Los indicadores clave de resultados no financieros deben aplicarse a cada uno de los apartados del estado de información no financiera. Estos indicadores deben ser útiles, teniendo en cuenta las circunstancias específicas y coherentes con los parámetros utilizados en sus procedimientos internos de gestión y evaluación de riesgos. En cualquier caso, la información presentada debe ser **precisa, comparable y verificable**.

Como se puede ver y es común, cada vez más, en el ámbito de la reflexión y de la ordenación de la gestión societaria, la concepción de la Ley que se acaba de

exponer parte de la propia consideración del proceso de gestión y- por tanto- de **adecuación de su marco jurídico** y del cumplimiento de las obligaciones que procedan- y de la identificación de los riesgos relacione. Este planteamiento es, ciertamente abierto y está en función del propio margen de actuación, del objeto social y del propio proceso de producción. Esta configuración se realiza sobre la base de los elementos generales de la entidad mercantil de que se trate y de la normativa sectorial del ámbito al que pertenezca la actividad realizada.

@@Actuación ejemplificativa del Instituto de Contabilidad y Auditoría de Cuentas (ICAC) y la Unión Europea

El carácter y la configuración abierta y en función de sus propios procesos de funcionamiento está admitido en las normas o reglamentaciones de uno u otro tipo que se han ido dictando para **clarificar la propia figura del informe no financiero**. Analizamos, seguidamente la posición del ICAC, en el ámbito de la Administración Española y de la propia Comisión Europea.

@@@ICAC

El ICAC tiene publicada una denominada “Guía informativa sobre la aplicación de la [Ley 11/2018, de 28 de diciembre, por la que se modifica el código de comercio](#), el texto refundido de la ley de sociedades de capital aprobado por el real decreto legislativo 1/2010, de 2 de julio [Ver], y la Ley 22/2015, de 20 de julio, de auditoría de cuentas, en materia de información no financiera y diversidad [Ver]”<sup>6</sup>.

Se contienen en esta Guía un conjunto de determinaciones que se asemejan a lo que venía analizando la Comisión Europea y que analizamos en el apartado siguiente.

En síntesis, se trata de determinar en este **Instrumento** orientativo la **obligación de presentación y algunas características del contenido del Informe** que, está basado, fundamentalmente, en la propia evaluación de los riesgos para la organización en concreto y de las medidas adoptadas para su prevención. El ICAC resalta, desde el principio, que los **elementos** que expresamente están citados en la regulación legal **no son taxativos**. Específicamente sobre este apartado, señala que «...9. *¿Es posible incluir información adicional a la exigida por la Ley? Sí. La Ley establece unos **requerimientos mínimos de información no financiera, pero no de máximos**. Por ello, todas aquellas empresas que ya incluían aspectos adicionales a los exigidos por la ley, o desean empezar a recogerlos, podrán continuar haciéndolo en la medida en que sean significativos y comprenda información concisa y útil que permita cumplir con la finalidad de la Ley...»<sup>7</sup>.*

En este contexto y teniendo en cuenta que existe una posición evidente de la **propia organización en la identificación de los riesgos de sus procesos y de su actividad** desde los parámetros identificados en la norma y aquellos otros que son consustanciales a la actividad y que pueden conllevar elementos adicionales que se diseñan en la propia norma y que son exigibles en dicho ámbito de actuación<sup>8</sup>.

En términos materiales respecto de su presentación se indica que «...Por su parte, el [artículo 49.6](#) del [Código de Comercio](#) (al que se remite el [262.5 TRLSC<sup>9</sup>](#)), prevé en su último párrafo que “*La información incluida en el estado de información no financiera será verificada por un prestador independiente de servicios de verificación.*”

Una interpretación sistemática de la remisión del [artículo 262.5](#) del [TRLSC](#) al [artículo 49.6](#) del [Código de Comercio](#), conforme al contexto, antecedentes y al espíritu y finalidad de la norma, llevan a la conclusión de que el legislador ha pretendido que toda la **regulación exigible para información no financiera**, incluida la de verificación independiente y el hecho de que la información no financiera sea un punto separado del orden del día, se aplique tanto a los grupos como a las sociedades de capital individuales, incluidas en el ámbito de aplicación de la [Ley 11/2018, de 28 de diciembre](#)...

## Comisión Europea

La Comisión Europea publica con la referencia 2017/C 215/01 unas **Directrices** sobre la **presentación** de informes no financieros<sup>10</sup>.

El apartado 3 contiene los principios fundamentales que pueden ser resumidos en los siguientes:

- Divulgación de **información significativa**
- Información, **fiel, equilibrada y comprensible**
- Información **completa** pero concisa
- Información **estratégica y prospectiva**
- Información orientada a las **partes interesadas**
- Información **coherente y sistemática**

Posteriormente cuando desarrolla el contenido del Informe, las Directrices parten de una **breve descripción** del negocio y su modelo y la evolución de las políticas de diligencia debida y los resultados de la aplicación de dicha política junto con la definición de los principales riesgos y su gestión y los indicadores de resultados.

*Específicamente y en relación con el respeto a los **derechos humanos** se señala que «...Se considera práctica recomendada para una sociedad el expresar su compromiso con el respeto de los derechos humanos. Este compromiso puede definir lo que una sociedad espera de su dirección, sus empleados y sus socios comerciales en términos de derechos humanos, incluidas normas fundamentales en materia laboral.*

La **información** puede explicar a los **derechos** de quiénes se refiere el compromiso, por ejemplo, los derechos de los niños, las mujeres, los pueblos indígenas, las personas con discapacidades, las comunidades locales, los agricultores minifundistas o las víctimas de la trata de seres humanos; y los derechos de los trabajadores, incluidos los que trabajan con contrato temporal, los trabajadores de los proveedores o los subcontratistas, los trabajadores migrantes y sus familias.

Las sociedades deben plantearse divulgar **información significativa** sobre la diligencia debida en materia de derechos humanos y sobre los procedimientos y disposiciones aplicados para **impedir los abusos** contra los derechos humanos. Esto puede incluir, por ejemplo, la manera en que se tratan las cuestiones de derechos humanos en los contratos de una sociedad con sus empresas proveedoras, y cómo mitiga la sociedad los potenciales efectos negativos en los derechos humanos y proporciona vías de reparación adecuadas si se han producido violaciones de estos derechos.

La información significativa divulgada puede reflejar cómo aborda una sociedad, entre otras cosas, los Principios Rectores sobre las empresas y los derechos humanos que ponen en práctica el marco de las Naciones Unidas para «proteger, respetar y remediar», las Líneas Directrices de la OCDE para Empresas Multinacionales, y la Declaración tripartita de **principios** sobre las empresas multinacionales y la política social, de la OIT»<sup>11</sup>.

## Tratamiento de la información y los riesgos de afección a los derechos fundamentales

Los apartados anteriores diseñan un **marco** en el que el concepto de informe no financiero adopta un **contenido flexible**, con inclusión **obligatoria** de determinadas materias, pero con la potencialidad de que, en función, de los riesgos a los bienes fijados se produzcan procesos diferentes de afección que determinan una posición activa susceptible de ser rendida en el marco de dicho instrumento, especialmente, cuando dicha inclusión y los procesos de prevención y cuidado puedan llegar a tener un valor de afección a un derecho fundamental.

Pues bien, en este marco podemos analizar que la protección y la ordenación de **una adecuada política relativa a la información** que maneja una organización es, sin duda, un elemento clave, desde la perspectiva de los derechos humanos.

En este punto, el [artículo 12](#) de la [Declaración Universal de Derechos Humanos de 1948](#)<sup>12</sup>, el [artículo 8](#) del Convenio para la protección de los derechos humanos y de las libertades fundamentales de 1950 [[Ver](#)]<sup>13</sup> y el propio [artículo 18](#) de [nuestra Constitución](#) (CE) establecen un **marco de privacidad** de contenido ciertamente amplio y que se refiere a un conjunto de ámbitos de actuación que se nuclean por su vinculación con la persona y con el ámbito en el que desarrolla su actividad. La privacidad es, por tanto, un ámbito o una **esfera de libertad de actuación no sometida a intromisiones** ni afecciones no queridas y no previstas en el Ordenamiento Jurídico.

El ámbito material de dicha privacidad es **amplio** y, realmente, conforma un esquema que no puede ser definido ni a priori ni delimitado con carácter general porque depende de muchos elementos que tienen que ver con el contenido objetivo y con los elementos externos que pueden afectarlo y estos dos factores están, muy a menudo, en una relación compleja y cambiante según los contextos sociales.

Conviene señalar, desde el principio, que la **protección** de los derechos fundamentales no opera únicamente en relación con las Administraciones Públicas sino, también, en las relaciones interprivados<sup>14</sup>.

La **jurisprudencia constitucional** ha resaltado y conceptualizado lo que acabamos de indicar. Esta formulación general puede verse desde la

[Sentencia del Tribunal Constitucional \(STC\) de 28 de enero de 2003](#), cuando establece que: «...*Delimitadas en los términos expuestos las posiciones de las partes, ha de traerse a colación la doctrina de este Tribunal, según la cual los derechos al honor, a la intimidad personal y a la propia imagen, reconocidos en el [art. 18.1 CE](#), a pesar de su estrecha relación en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un **contenido propio y específico**. Se trata, dicho con otras palabras, de derechos autónomos, de modo que, al tener cada uno de ellos su propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás ([SSTC 81/2001, de 26 de marzo, F. 2; 156/2001, de 2 de julio, F. 3](#)).*»

*Como hemos declarado en la última de las Sentencias citadas, el **carácter autónomo** de los derechos del [art. 18.1 CE](#) supone que ninguno de ellos tiene respecto de los demás la consideración de derecho genérico que pueda subsumirse en los otros dos derechos fundamentales que prevé este precepto constitucional, pues la **especificidad** de cada uno de estos derechos impide considerar subsumido en alguno de ellos las vulneraciones de los otros derechos que puedan ocasionarse a través de una imagen que muestre, además de los rasgos físicos que permiten la identificación de la persona, aspectos de su vida privada, partes íntimas de su cuerpo o que se la represente en una situación que pueda hacer desmerecer su buen nombre o su propia estima.*

*En tales supuestos la apreciación de la vulneración del derecho a la imagen no impedirá, en su caso, la apreciación de la vulneración de las eventuales lesiones del derecho a la intimidad o al honor que a través de la imagen se hayan podido causar, pues, desde la perspectiva constitucional, el desvalor de la acción no es el mismo cuando los hechos realizados sólo pueden considerarse lesivos del derecho a la imagen que cuando, además, a través de la imagen puede vulnerarse también el derecho al honor o a la intimidad, o ambos derechos conjuntamente (F. 3; en el mismo sentido, [SSTC 81/2001, de 26 de marzo, F. 2; 83/2002, de 22 de abril, F. 4](#))....». En un momento final, la propia sentencia señala que «...El **derecho al olvido**, como todo derecho fundamental, no es ilimitado, y encuentra sus límites en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos ([STC 58/2018](#), FJ 6)....».*

Este ámbito se ha ido **extendiendo** a momentos en los que la propia persona ha dejado de existir o cuando la situación se hace desproporcionada en relación con la actualidad del momento y de las circunstancias en las que se produce la conservación de la información.

Convencionalmente hemos dado en llamar a esta segunda cuestión como **derecho al olvido**.<sup>15</sup> La [STC de 29 de junio de 2022](#) lo define en los siguientes términos: «...*El ejercicio del derecho al olvido, anudado a la voluntad de su titular de controlar el uso de sus datos, aparece actualmente regulado en el [art. 17 RGPD](#)<sup>16</sup>, al que remite expresamente el [art. 15.1](#) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). [Ver] Este precepto establece **seis circunstancias que hacen nacer el derecho de supresión o derecho al olvido**, en concreto, cuando:*

- i) los datos personales ya **no sean necesarios** en relación con los fines para los que fueron recogidos o tratados;
- ii) el interesado **retire el consentimiento** en que se basó el tratamiento;
- iii) el interesado **se oponga** al tratamiento;
- iv) los datos personales hayan sido **tratados ilícitamente**;
- v) los datos personales **deban suprimirse** para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros; y,
- vi) los datos personales se hayan **obtenido** en relación con la **oferta de servicios de la sociedad de la información**.

*El [Reglamento General de Protección de Datos](#) era aplicable únicamente a partir del 25 de mayo de 2018 ([art. 99.2 RGPD](#)), por lo que no cabe su aplicación en el presente supuesto dado que la resolución de la AEPD es de fecha 16 de marzo de 2017. No obstante, como también advertimos en la [STC 58/2018](#), FJ 5, el derecho al olvido **ya existía** por obra de la [Directiva 95/46/CE](#), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante [Directiva 95/46](#)), en la interpretación que la [STJUE Google Spain \(TJCE 2014, 85\)](#), dio a los [arts. 12, b\)](#) y [14.1 a\)](#) de dicha [Directiva](#)...».*

El marco al que acabamos de hacer referencia se ha completado, en el plano jurisprudencial, con la conformación del **derecho a la protección de datos**. Se trata de una esfera diferencial, vinculada a la técnica y a la tecnología y a la forma en que se configuran los derechos de la persona en el marco de las relaciones jurídicas. Como referencia de esta doctrina nos vale el resumen que efectúa la [STC 89/2022, de 29 de junio](#) cuando señala que:

*«...El **objeto del derecho fundamental** a la protección de datos personales "no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales" ([STC 292/2000, de 30 de noviembre](#), FJ 6), y, en cuanto a su contenido, atribuye a su titular "un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer" ([SSTC 96/2012, de 7 de mayo](#), FJ 7 y [292/2000](#), FJ 6). De esta manera el derecho al olvido, entendido como un derecho a la supresión del uso o*

*tratamiento de los datos personales, alcanza a todos los datos relativos a la identificación de una persona, incluso aunque no afecten a su honor, intimidad personal y familiar o a la propia imagen. Se reconoce así a la persona un **poder de disposición** sobre sus datos, que, a la postre, determina también la posibilidad de pedir la supresión del tratamiento que se haga con los mismos en determinadas circunstancias...».*

Llegados a este punto podemos indicar que existen diferentes supuestos en los que los datos personales, la información y su régimen jurídico vertebran la **protección jurídica sustantiva** de los derechos. De esta forma podríamos decir que el cumplimiento de la regularidad de la información es parte de la protección del derecho en cuestión.

Desde esta perspectiva la afección a los derechos de la persona y a su esfera de intimidad está **vinculado** a la regularidad de la aplicación del régimen jurídico respectivo.

A partir de esta afirmación podríamos decir que existe un conjunto disperso de **normas que regulan la producción de información**, su conservación o archivo y, finalmente, su destrucción.

Este régimen es diversos en función de criterios diversos que se corresponden, en unos casos, con la **perspectiva subjetiva** del custodio de los documentos y en otras con la actividad material y la regulación sectorial de la misma que se realiza.

# Algunas referencias a la destrucción de la información como elemento de preservación de valores diversos legalmente asumidos

## Normativa administrativa

- De carácter general

Básicamente y al margen de algunas referencias relativas a los registros y archivos que se contienen en las leyes administrativas de carácter general (nos referimos esencialmente a las [Leyes 39/2015](#) y [40/2015](#)) es el Real Decreto 1708/2011, de 18 de noviembre, la norma que establece el sistema español de archivos y se regula el sistema de archivos de la Administración General del Estado. [\[Ver\]](#)

En el capítulo III del citado [Real Decreto 1708/2011](#) se regula el **régimen de archivos** diferenciando entre los **archivos de oficina o de gestión**<sup>17</sup>, los **archivos generales** o centrales de los ministerios y de los Organismos Públicos<sup>18</sup> y el **archivo intermedio** que «...es la institución responsable de la custodia de los documentos generados y reunidos por los diferentes Departamentos ministeriales y sus organismos públicos, una vez finalizada su fase

*activa conforme a lo establecido en los calendarios de conservación. El Archivo General de la Administración, es el archivo intermedio de la Administración General del Estado, según la normativa vigente...»* y que concluye con la regulación del **archivo histórico**<sup>19</sup>.

Más allá del plano orgánico, la destrucción de la información exige la **evaluación documental** que es una síntesis entre la habilitación legal de carácter sectorial para la realización de esta actividad y la del valor general en el ámbito de la valoración o el interés histórico, documental, estadístico y demás que pueden exigir la conservación in natura o en un soporte diferencial a la inicial.

- Las referencias por vinculación con el concepto y la protección de los datos personales

Esta norma contiene referencias ineludibles a la información y su disponibilidad. En esencia, la regulación se encuentra en el [artículo 32](#) de la [LOPD](#) cuando señala que:

#### a) Regla general

Es la prevista en el [apartado 1](#) según la cual «...1. El responsable del tratamiento estará obligado a **bloquear los datos** cuando proceda a su **rectificación o supresión**...». Este precepto, como se ve, introduce la referencia a la supresión de la información y la forma de su realización.

#### b) Contenido formal del bloqueo

Está contenido en el [apartado 2](#) cuando señala que:

*«...2. El bloqueo de los datos consiste en 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 solo por el plazo de prescripción de las mismas.*

Transcurrido ese plazo deberá procederse a la destrucción de los datos...»

Como puede verse se trata de un conjunto de **características técnicas** que operan en el plano finalista de impedir el tratamiento de las mismas y con inclusión en este apartado de la referencia a la visualización con excepción, en este caso, al cumplimiento de las obligaciones en el orden de las responsabilidades públicas y de orden penal.

#### c) Consecuencia del bloqueo

Es la prevista en el [apartado 3](#) del propio artículo cuando señala que «...3. Los datos bloqueados **no podrán ser tratados** para ninguna finalidad distinta de la señalada en el apartado anterior...».

## Ejemplos de leyes de ámbito general que se

# proyectan sobre el régimen jurídico de la conservación documental

Sin ninguna pretensión de exhaustividad sino únicamente de la fijación de algunos **ejemplos** que puedan servir para fundar una **doctrina general sobre la obligación de destrucción de la documentación** como parte del régimen jurídico de determinadas relaciones jurídicas. Esta determinación tiene diversos fundamentos que van desde la innecesaridad hasta la obligación expresa para la protección de intimidad de la relación en cuestión. Veamos algunos ejemplos:

## Ley General Tributaria

El [artículo 29](#) de la [Ley 58/2003, de 17 de diciembre, General Tributaria \(LGT\)](#) configura como **obligación tributaria formal** la de:

d) La **obligación de llevar y conservar libros de contabilidad** y registros, así como los programas, ficheros y archivos informáticos que les sirvan de soporte y los sistemas de codificación utilizados que permitan la interpretación de los datos cuando la obligación se cumpla con utilización de sistemas informáticos. Se deberá facilitar la conversión de dichos datos a **formato legible** cuando la lectura o interpretación de los mismos no fuera posible por estar encriptados o codificados.

En todo caso, los obligados tributarios que deban presentar autoliquidaciones o declaraciones por **medios telemáticos** deberán conservar copia de los programas, ficheros y archivos generados que contengan los datos originarios de los que deriven los estados contables y las autoliquidaciones o declaraciones presentadas

Dicha determinación se compagina en el [artículo 66](#) de la [LGT](#) con la **fijación de los plazos de prescripción** que, claro está, al no ser ya parte de una obligación exigible tiene la consideración y el efecto de hacer decaer el deber de custodia tanto de la Administración, claro está, como, igualmente, de los particulares<sup>20</sup>. Estos efectos están claramente expuesto en el [artículo 69](#) de la [LGT](#) que, precisamente, se refiere a la **extensión y efectos de la prescripción**<sup>21</sup>.

Este esquema nos sirve para señalar un **modelo de actuación** que consiste en no indicar ni regular específicamente un plazo de expurgo de la documentación pero si de establecer un **plazo de prescripción** fuera del cual la utilización de la información está pendiente únicamente de que no exista una decisión administrativa de expurgo o destrucción que pasa a responder a criterios de gestión y organización pero que, evidentemente, carece de efectos en el marco de las relaciones jurídicas que contiene.

## Ley 41/2002, de 14 de noviembre, básica

# reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica

En su Capítulo V la [Ley 41/2002 se refiere a la historia clínica](#). Es el [artículo 14](#) el que señala que:

1. La **historia clínica comprende** el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la **documentación clínica de cada paciente**, al menos, en el ámbito de cada centro.

2. Cada centro **archivará** las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información...

Al lado de esta determinación que se mueve en el plano delimitativo se añade, en el [artículo 16](#), lo relativo a los usos indicando que:

“La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia...”

Finalmente, el [artículo 17](#) se refiere, directamente, a la **conservación de la documentación clínica** indicando que:

Los centros sanitarios tienen la **obligación de conservar** la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, **cinco años** contados desde la fecha del alta de cada proceso asistencial...

. Esta **habilitación temporal** se completa con una referida a determinados datos clínicos y que concluye con la referencia a que no se destruirán los «...los datos de la historia clínica relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración correspondiente, donde se conservarán con las debidas medidas de seguridad a los efectos de la legislación de protección de datos...»

Es este un tipo de **regulación sectorial** – pensada, incluso, en clave de destinatarios múltiples que son los que componen el sistema sanitario en el que se determina el concepto de

información, el plazo de conservación y, eventualmente, los posibles usos de la misma.

Cuando nos encontramos con una sectorial tan detallada los preceptos y los **conceptos generales** que hemos apuntado en el marco de las grandes leyes administrativas ganan todo su sentido porque a las determinaciones generales que establecen éstas se unen las **concretas y determinadas de la legislación sectorial aplicable**. Una determinación de este orden que implica un esquema de facilidad en la interpretación sistemática de las normas nos permite señalar un ejemplo que realmente demuestra la utilidad del esquema legislación general-legislación especial y las carencias que supone la ruptura del binomio al que nos referimos.

## Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad del Estado en lugares públicos

El [artículo 8](#) de la [Ley Orgánica 4/1997](#), en otro ejemplo quizá más contundente, señala que:

Las grabaciones serán **destruidas** en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto...<sup>22</sup>

## Ley de Seguridad Aérea

Por poner otro ejemplo, la [Ley 21/2003, de 7 de julio, de Seguridad Aérea](#) (LSA) contiene un régimen que podemos sintetizar en la forma que se expone en los apartados que siguen.

El [artículo 18.1](#) de la [LSA](#) establece que:

Los **datos**, registros, grabaciones, declaraciones, comunicaciones, indicadores e informes **facilitados en el marco del Programa Estatal de Seguridad Operacional para la Aviación Civil** por los profesionales aeronáuticos y proveedores de servicios y productos aeronáuticos a los organismos, órganos, entes y entidades del sector público a que se refiere el [artículo 11.3](#), párrafo primero, tienen carácter reservado y sólo pueden ser utilizados para los fines previstos en él.

El **deber de reserva** en relación con la información obtenida en la investigación técnica de los accidentes o incidentes en la aviación civil se regirá por lo previsto en el Reglamento (UE) n.º 996/2010 del Parlamento Europeo y del Consejo, de 20 de octubre de 2010. [\[Ver\]](#)

En todo caso, la información a que se refieren los párrafos anteriores se recaba con

la única **finalidad de reforzar la seguridad operacional** y prevenir futuros accidentes e incidentes, y no con la finalidad de determinar culpas o responsabilidades...

Lo característico de esta determinación es que va seguida, en el propio artículo, con la indicación del **deber de reserva de las personas que conozcan de esta información**<sup>23</sup>.

El marco de la documentación es, como hemos visto en otros ejemplos, el de la prescripción que, en este caso se contiene en el [artículo 60](#), en estos términos:

1. Las **infracciones administrativas** previstas en esta ley prescribirán en el plazo de tres años las muy graves, en el de dos años las graves y en el de un año las leves.
2. Las sanciones impuestas por la comisión de **infracciones muy graves** prescribirán a los tres años, en tanto que las impuestas por graves o leves lo harán a los dos años y al año, respectivamente.
3. Para el cómputo de los plazos de prescripción de infracciones y sanciones se estará a lo dispuesto en el [artículo 132. 2 y 3](#) de la [Ley 30/1992](#).

En los supuestos de infracciones continuadas, el plazo de prescripción comenzará a contar desde el momento de la finalización de la actividad o del último acto con el que la infracción se consuma. En el caso de que los hechos o actividades constitutivos de infracción fueran desconocidos por carecer de signos externos, dicho plazo se computará desde que éstos se manifiesten...

## Las políticas de borrado y destrucción de la información como parte de la garantía de la correcta utilización y del cumplimiento de las obligaciones en dicho ámbito

Las referencias que acaban de indicarse, situadas, como hemos dicho, en el plano del ejemplo, nos presenta un conjunto de ordenaciones que establecen el **régimen jurídico de la información**. En la expresión «*régimen jurídico de la información*» subyace la protección de un conjunto de valores que, en unos casos, son de pura ordenación administrativa y, ligados, por tanto, al régimen de la actuación administrativa y, en otros, tienden a asegurar que los derechos y valores ínsitos en la ordenación de la información sirven para asegurar el régimen del derecho subyacente.

En este sentido, cuando la información en cuestión afecta al **ámbito de privacidad**, a la intimidad de las personas o al derecho a la protección de datos – al que ya nos hemos referido – su destrucción es una garantía del ejercicio de los derechos de la persona porque, precisamente, lo que resulta determinante es indicar que la **destrucción es una obligación**

**legal** y, sobre todo, una **garantía** que conecta directamente con el núcleo esencial de los derechos de la persona en su propia delimitación legal. Conviene recordar, en este punto y como hemos señalado, la doctrina constitucional plasmada, entre otras, en la [STC 177/1988, de 30 de octubre](#) cuando señala que:

*«...De aquí que este Tribunal haya reconocido que los actos privados puedan lesionar los derechos fundamentales y que en estos supuestos los interesados pueden acceder a la vía de amparo si no obtienen la debida protección de los Jueces y Tribunales a los que el ordenamiento encomienda la tutela general de los mismos. Las relaciones entre particulares, si bien con ciertas matizaciones, no quedan, pues, excluidas del ámbito de aplicación del principio de igualdad, y la autonomía de las partes ha de respetar tanto el principio constitucional de no discriminación como aquellas reglas, de rango constitucional u ordinario, de las que se derive la necesidad de igualdad de trato. No cabe olvidar que el [art. 1.1 C. E.](#) propugna entre los valores superiores del ordenamiento jurídico la igualdad, y que el [9.2](#) encomienda a todos los poderes públicos promover las condiciones para que la igualdad del individuo y de los grupos en que se integra sean reales y efectivas...».*

Situados en este plano cabe indicar que cuando el [artículo 44](#) del [Código de Comercio](#) se refiere a la **protección de derechos humanos**, o de derechos de la persona está determinando que la organización en cuestión debería demostrar cual es el procedimiento de destrucción que resulta aplicable para asegurar el derecho a la privacidad que subyace en dicho ámbito. La **intervención de la entidad privada** deriva, por tanto, de la obligación de que su actuación respete el marco de protección que enlaza directamente con la preservación de la privacidad y de la intimidad. Este derecho tiene una faceta activa de establecimiento de un marco de protección que incluye las **garantías frente a terceros** de que, cuando lo determine la legislación aplicable, los elementos que pueden afectar al ámbito de la privacidad sean destruido en forma que, técnicamente, se asegure la imposibilidad de recuperación y, por tanto, de potencial violación posterior.

En este punto lo que conviene indicar, como elemento central, es que el **aseguramiento de la destrucción de la información** – cualquiera que sea el soporte material en el que se contenga aquella- es un elemento conceptual ligado a la utilización y ejercicio de los derechos y a la prevención de que la esfera de intimidad y de privacidad en la que se sitúa no son o no resultan afectados como consecuencia de una mala praxis en la fase final de la documentación o de formalización de la esfera de intimidad que los mismos significan.

Esto ha llevado a una preocupación central sobre el aseguramiento que se traduce, como señalábamos, al **principio en un compromiso de estandarización** que, en esencia, se vincula a los siguientes **instrumentos**:

- **SO/IEC 27001**: Norma internacional de seguridad de la información que establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).
- **ISO/IEC 27040**: Guía para la aplicación de la ISO/IEC 27001 en el sector de las tecnologías de la información y las comunicaciones (TIC).

Estas normas establecen que los **datos personales deben ser borrados de forma segura y**

**efectiva**, de manera que no puedan ser recuperados. Para ello, se deben utilizar métodos de borrado que garanticen la destrucción irreversible de los datos, como el borrado por sobrescritura, el borrado por desmagnetización o el borrado físico.

Este esfuerzo de estandarización encuentra, pronto, una referencia normativa más amplia ya en el plano normativo y del que podemos referirnos a los siguientes **hitos normativos**:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: [\[Ver\]](#) Esta directiva establece el **marco general** para la **protección de datos personales en la Unión Europea**. En su [artículo 12](#), establece que los datos personales deben ser borrados cuando ya no sean necesarios para los fines para los que fueron recogidos o tratados.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas [\[Ver\]](#) ([Directiva sobre la privacidad y las comunicaciones electrónicas](#)): Esta directiva establece **normas específicas para la protección de datos personales en el sector de las comunicaciones electrónicas**. En su [artículo 15](#), establece que los usuarios tienen derecho a solicitar a los proveedores de servicios de comunicaciones electrónicas que borren sus datos personales.

En España, la **acreditación ISO** es regulada por la Entidad Nacional de Acreditación (ENAC), que es el **organismo nacional** de acreditación designado por el Ministerio de Industria, Comercio y Turismo. La ENAC está acreditada por la IAF, lo que significa que cumple con los requisitos internacionales para la acreditación<sup>24</sup>.

La ENAC **acredita a los organismos de evaluación** que cumplen con los requisitos de las normas ISO/IEC 17011. Estos organismos pueden ser laboratorios de ensayo, laboratorios de calibración, organismos de inspección, organismos de certificación, o cualquier otro tipo de organismo que realice actividades de evaluación.

El **proceso de acreditación ISO** es un proceso complejo que requiere que el organismo de evaluación demuestre su competencia técnica, su imparcialidad y su independencia. El proceso de acreditación se lleva a cabo por un equipo de auditores independientes que evalúan al organismo de evaluación en su totalidad.

Los organismos de evaluación acreditados por la ENAC pueden ofrecer sus servicios a empresas, organizaciones e instituciones de todo el mundo. La acreditación ISO **proporciona a los clientes una garantía de que los servicios de evaluación** que reciben cumplen con los requisitos internacionales de calidad.

En resumen, la acreditación ISO es un proceso que se regula a nivel internacional por la IAF y a nivel nacional por los organismos nacionales de acreditación, como la ENAC en España. La acreditación ISO proporciona una garantía de que los organismos de evaluación que **cumplen con los requisitos** de las normas ISO/IEC 17011 son competentes, imparciales e independientes.

Adicionalmente y para los productos debe tenerse en cuenta lo previsto en Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, [Ver] entre cuyas **competencias** se encuentra:

«...Constituir el **organismo de certificación** del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito. d) **Valorar y acreditar la capacidad de los productos** de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura...».

Esto nos permite indicar que la acreditación de las empresas y de los productos responde, esencialmente, a un marco de estandarización que aplican empresas acreditadas por los órganos nacionales de acreditación o con competencia en la materia.

Llegados a este punto cabe indicar que la **aportación de estos esquemas de aseguramiento** de la destrucción de la información, en el momento que, respectivamente, establezcan las leyes se convierte en un elemento clave para demostrar que se produce un **adecuado tratamiento de la información** que afecta a la esfera de privacidad de las personas<sup>25</sup>.

Cuando llegamos a este punto, la consecuencia lógica es evidente: en el informe a que se refiere el [artículo 44](#) del [Código de Comercio](#) debe **justificarse el sistema de destrucción** por el que opta la correspondiente organización es segura en los términos convencionales que se produce este aseguramiento en la sociedad actual que es mediante el **sometimiento** de las empresas, sus procedimientos y sus productos a **esquemas de acreditación y validación** conforme a esquemas de estandarización internacionales.

Esto nos lleva a la conclusión de que las **técnicas de destrucción de la información** deben figurar en el **marco** del conjunto de reflexiones y de identificaciones de riesgos que las empresas deben realizar y que hemos agrupados en torno al denominado Informe no financiero. Es cierto, claro está, que su incorporación lo es en los términos comunes de identificación del riesgo y de exposición de las medidas utilizadas y no, claro está, con una capacidad de ordenación coercitiva como ocurre en el marco de las normas de carácter sancionador.

[1] Es de referencia la monografía de ÁLVAREZ GARCÍA, V., La normalización industrial, Tirant lo blanch, Valencia, 1999.

[2] La Directiva señala que «...La necesidad de mejorar la divulgación de información de contenido social y medioambiental por parte de las empresas, mediante la presentación de una propuesta legislativa en este ámbito, se reiteró en la Comunicación de la Comisión titulada «Estrategia renovada de la UE para 2011-2014 sobre la responsabilidad social de las empresas», adoptada el 25 de octubre de 2011...»

[3] En otro momento, se señala que «...En caso de que se exija a las empresas la elaboración de un estado no financiero, dicho estado debe incluir, en lo que atañe a cuestiones medioambientales, información detallada sobre los efectos actuales y previsibles de las actividades de la empresa en el medio ambiente, y, en su caso, la salud y la seguridad, el uso de energía renovable y/o no renovable, las emisiones de gases de efecto invernadero, el

consumo de agua y la contaminación atmosférica. Por lo que respecta a las cuestiones sociales y relativas al personal, la información facilitada en el estado puede hacer referencia a las medidas adoptadas para garantizar la igualdad de género, la aplicación de convenios fundamentales de la Organización Internacional del Trabajo, las condiciones de trabajo, el diálogo social, el respeto del derecho de los trabajadores a ser informados y consultados, el respeto de los derechos sindicales, la salud y seguridad en el lugar de trabajo y el diálogo con las comunidades locales, y/o las medidas adoptadas para garantizar la protección y el desarrollo de esas comunidades. Por lo que se refiere a los derechos humanos, a la lucha contra la corrupción y al soborno, el estado no financiero podría incluir información sobre la prevención de las violaciones de los derechos humanos y/o sobre los instrumentos existentes para luchar contra la corrupción y el soborno...».

[4] A esta cuestión nos referimos en CAMPUZANO, A.B, y PALOMAR OLMEDA, A., “El informe de información no financiera: evolución e incidencia en la ley de Cambio Climático y en el ámbito de la gestión administrativa”, Revista Aranzadi de Derecho Ambiental, núm. 49, 2021, especialmente pp. 32-44. Pueden consultarse también, con más detalle, los trabajos de ENCISO ALONSO-MUÑUMER, M., “TRANSPARENCIA Y SOSTENIBILIDAD”, Revista de Derecho del Mercado de Valores, núm. 27, 2020, pp. 242-281, y FERNÁNDEZ-RAÑADA, J., “El estado de información no financiera”, Comunicaciones en Propiedad Industrial y Derecho de la Competencia, núm. 88, 2019, pp. 157-166.

[5] En relación con esta categoría específica el apartado 2 señala que «...se da nueva redacción al apartado 5 y se añaden cuatro nuevos apartados 6, 7, 8 y 9 en el artículo 49, que quedan redactados como sigue: «5. Las sociedades que formulen cuentas consolidadas, deberán incluir en el informe de gestión consolidado el estado de información no financiera consolidado previsto en este apartado siempre que concurren los siguientes requisitos: a) Que el número medio de trabajadores empleados por las sociedades del grupo durante el ejercicio sea superior a 500. b) Que o bien, tengan la consideración de entidades de interés público de conformidad con la legislación de auditoría de cuentas, o bien, durante dos ejercicios consecutivos reúnan, a la fecha de cierre de cada uno de ellos, al menos dos de las circunstancias siguientes: 1.º Que el total de las partidas del activo consolidado sea superior a 20.000.000 de euros. 2.º Que el importe neto de la cifra anual de negocios consolidada supere los 40.000.000 de euros. 3.º Que el número medio de trabajadores empleados durante el ejercicio sea superior a doscientos cincuenta...».

[6] Disponible en: <https://www.icac.gob.es/node/1723> (último acceso: 2 de febrero de 2024).

[7] Ibidem, p. 9.

[8] La Guía detalla las reglas de la evaluación indicando que: «...6.1.- Opinión técnica: la opinión deberá expresarse en términos de seguridad razonable o limitada, u otra, según se opte. – (seguridad razonable) Una opinión técnica en la que se manifestará, de forma clara y precisa, si el EINF se ha presentado en todos sus aspectos significativos de conformidad con lo establecido en el marco legal aplicable ([artículo 49.6 del Código de Comercio](#), [artículo 262.5 del TRLSC](#) o normas de desarrollo). – (seguridad limitada) Una opinión en la que se indique que en base a los procedimientos aplicados y la evidencia obtenida, no ha llegado a conocimiento del verificador ninguna cuestión que le lleve a pensar que el EINF no se ha presentado en todos sus aspectos significativos de conformidad con lo establecido en el marco legal aplicable

([artículo 44.6](#) del [Código de Comercio](#), el [artículo 262.5](#) del texto refundido de la [Ley de Sociedades de Capital](#) o normas de desarrollo). – (otra) En el caso de tratarse de otro tipo de seguridad, se deberá manifestar expresamente cuál es la conclusión alcanzada y el alcance de las pruebas planificadas y realizadas que han servido de base para dicha conclusión.

[9] El acrónimo corresponde al Texto Refundido de la [Ley de sociedades de capital](#) aprobado por el [Real Decreto Legislativo 1/2010](#), de 2 de julio.

[10] Publicadas en el Diario Oficial de la Unión Europea, núm. C 215, de 5 de julio de 2017, pp. 1-20.

[11] Las determinaciones sobre los derechos humanos se completan con la siguiente referencia: «...Ejemplo e indicadores clave de resultados Una sociedad puede divulgar información significativa e indicadores clave de resultados sobre: —frecuencia con que se producen repercusiones graves sobre los derechos humanos en relación con sus actividades o decisiones, —procedimiento para la presentación y el tratamiento de denuncias y para mitigar las violaciones de derechos humanos y proporcionar reparación a sus víctimas, —actividades y proveedores expuestos a un riesgo significativo de sufrir violaciones de los derechos humanos, —procedimientos y medidas para prevenir la trata de seres humanos, para todas las formas de explotación, trabajo forzado u obligatorio y trabajo infantil, trabajo precario y condiciones de trabajo inseguras, en particular por lo que respecta a las zonas geográficas con mayor riesgo de exposición a abusos, —accesibilidad de sus instalaciones, documentos y páginas web para las personas con discapacidad, —respeto de la libertad de asociación, —cooperación con las partes interesadas pertinentes...».

[12] Señala que «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

[13] El citado artículo 8 establece que: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás...».

[14] En este sentido, la [STC 56/1995 de 6 de marzo](#) en la que se llega a afirmar que «...Este derecho, proclamado en el [art. 20 CE](#), es también en esencia, como la mayor parte de los derechos fundamentales, un derecho frente a los poderes públicos ([ATC 673/1985](#)). Sin embargo, este Tribunal ha reiterado que su contenido se extiende a las relaciones entre particulares y puede por tanto reivindicarse frente a este tipo de sujetos, aunque en este caso el contenido y ejercicio del derecho se someta a unos límites específicos ([SSTC 120/1983](#) [ RTC 1983\120], [88/1987](#) [ RTC 1987\88], [126/1990](#) [ RTC 1990\126], [286/1993](#) [ RTC 1993\286])...». En el mismo sentido, la [STC 18/1984 de 7 de febrero](#) cuando señala que «...Esta concretización de la Ley suprema no debe interpretarse en el sentido de que sólo se sea titular de los derechos fundamentales y libertades públicas en relación con los poderes públicos, dado que en un

Estado social de derecho como el que consagra el [artículo 1.º](#) de la [Constitución](#) no puede sostenerse con carácter general que el titular de tales derechos no lo sea en la vida social, tal y como evidencia la [Ley 62/1978](#), de Protección de los Derechos Fundamentales, la cual prevé la vía penal -aplicable cualquiera que sea el autor de la vulneración cuando cae dentro del ámbito penal-, la contencioso-administrativa -ampliada por la [disposición transitoria segunda](#), 2, de la [LOTC](#)- y la civil, no limitada por razón del sujeto autor de la lesión. Lo que sucede, de una parte, es que existen derechos que sólo se tienen frente a los poderes públicos (como los del [artículo 24](#)) y, de otra, que la sujeción de los poderes públicos a la [Constitución](#) (art. 9.1) se traduce en un deber positivo de dar efectividad a tales derechos en cuanto a su vigencia en la vida social, deber que afecta al legislador, al ejecutivo y a los Jueces y Tribunales, en el ámbito de sus funciones respectivas. De donde resulta que el recurso de amparo se configura como un remedio subsidiario de protección de los derechos y libertades fundamentales, cuando los poderes políticos han violado tal deber. Esta violación puede producirse respecto de las relaciones entre particulares cuando no cumplen su función de restablecimiento de los mismos, que normalmente corresponde a los Jueces y Tribunales, a los que el Ordenamiento encomienda la tutela general de tales libertades y derechos ([artículo 41.1](#) de la [LOTC](#)). En este sentido, debe recordarse que el Tribunal ha dictado ya sentencias en que ha admitido y fallado recursos de amparo contra resoluciones de órganos judiciales, cuando los actos sujetos al enjuiciamiento de los mismos provenían de particulares, debiendo ahora remitirnos a la doctrina sentada en nuestra sentencia de 29 de enero de 1982, número 2/1982 ( RTC 1982\2), acerca de las peculiaridades que presenta la competencia del Tribunal Constitucional cuando se impugna ante el mismo, en vía de amparo, resoluciones de órganos judiciales.

[15] Sobre esta cuestión contamos con aportaciones doctrinales en los trabajos, por todos, de ÁLVAREZ CARO, M., “El derecho a la supresión o al olvido”, [Reglamento general de protección de datos](#): hacia un nuevo modelo europeo de privacidad (Álvarez Caro, M., Recio Gayo, M. y Piñar Mañas, J.L.; Dirs.), Reus, Madrid, 2016, pp. 241-256; CASINO RUBIO, M., “El periódico de ayer, el derecho al olvido en internet y otras noticias”, *Revista Española de Derecho Administrativo*, núm. 156, 2012, pp. 201-216; ESTEPA MORENO, M., “La conformación del derecho al olvido en la protección de datos personales”, *Anuario Jurídico y Económico Escurialense*, núm. 56, 2023, pp. 37-58; GUICHOT REINA, E., “La publicidad de datos personales en internet por parte de las Administraciones Públicas y el derecho al olvido”, *Revista Española de Derecho Administrativo*, núm. 154, 2012, pp. 125-168, y SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital*, Tiran lo Blanch, Valencia, 2012.

[16] El acrónimo es para el [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](#) ([Reglamento general de protección de datos](#)).

[17] «...Son aquellos archivos existentes en todos los órganos y unidades administrativas para la custodia de los documentos en fase de tramitación o sometidos a continua utilización y consulta administrativa. Estos documentos, una vez concluida su tramitación o su etapa de utilización y consulta, serán objeto de transferencia al archivo central del Departamento respectivo, de acuerdo con los plazos establecidos durante el proceso de valoración...»

[18] El citado artículo 10 establece que «...Son aquellos archivos existentes en los Ministerios y

organismos públicos para la custodia de los documentos, una vez finalizada su tramitación y transcurridos los plazos establecidos por la normativa vigente o en los calendarios de conservación.»

[19] Su regulación se contiene en el artículo 12 cuando señala que «...conservación y tratamiento de los fondos pertenecientes al patrimonio histórico documental español que sean reflejo de la trayectoria de la administración estatal a lo largo de la historia o que en todo caso resulten altamente significativos por su valor histórico, su singular importancia o su proyección internacional. Son archivos históricos los de titularidad y gestión estatal adscritos al Ministerio de Cultura...»

[20] Este plazo tiene, sin embargo, una excepción prevista en el propio artículo 66 bis cuando señala que «...El derecho de la Administración para iniciar el procedimiento de comprobación de las bases o cuotas compensadas o pendientes de compensación o de deducciones aplicadas o pendientes de aplicación, prescribirá a los diez años a contar desde el día siguiente a aquel en que finalice el plazo reglamentario establecido para presentar la declaración o autoliquidación correspondiente al ejercicio o periodo impositivo en que se generó el derecho a compensar dichas bases o cuotas o a aplicar dichas deducciones. En los procedimientos de inspección de alcance general a que se refiere el artículo 148 de esta Ley, respecto de obligaciones tributarias y periodos cuyo derecho a liquidar no se encuentre prescrito, se entenderá incluida, en todo caso, la comprobación de la totalidad de las bases o cuotas pendientes de compensación o de las deducciones pendientes de aplicación, cuyo derecho a comprobar no haya prescrito de acuerdo con lo dispuesto en el párrafo anterior. En otro caso, deberá hacerse expresa mención a la inclusión, en el objeto del procedimiento, de la comprobación a que se refiere este apartado, con indicación de los ejercicios o periodos impositivos en que se generó el derecho a compensar las bases o cuotas o a aplicar las deducciones que van a ser objeto de comprobación. La comprobación a que se refiere este apartado y, en su caso, la corrección o regularización de bases o cuotas compensadas o pendientes de compensación o deducciones aplicadas o pendientes de aplicación respecto de las que no se hubiese producido la prescripción establecida en el párrafo primero, sólo podrá realizarse en el curso de procedimientos de comprobación relativos a obligaciones tributarias y periodos cuyo derecho a liquidar no se encuentre prescrito. 3. Salvo que la normativa propia de cada tributo establezca otra cosa, la limitación del derecho a comprobar a que se refiere el apartado anterior no afectará a la obligación de aportación de las liquidaciones o autoliquidaciones en que se incluyeron las bases, cuotas o deducciones y la contabilidad con ocasión de procedimientos de comprobación e investigación de ejercicios no prescritos en los que se produjeron las compensaciones o aplicaciones señaladas en dicho apartado.».

[21] El [artículo 69 LGT](#) establece que «...1. La prescripción ganada aprovecha por igual a todos los obligados al pago de la deuda tributaria salvo lo dispuesto en el apartado 8 del artículo anterior. 2. La prescripción se aplicará de oficio, incluso en los casos en que se haya pagado la deuda tributaria, sin necesidad de que la invoque o excepcione el obligado tributario. 3. La prescripción ganada extingue la deuda tributaria...».

[22] Esta determinación se completa con la indicación de que «...2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley. 3. Se prohíbe la cesión o copia de las

imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo. 4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados...».

[23] En punto a este deber de reserva se señala que: «...3. El incumplimiento del deber de reserva regulado en este artículo determinará las responsabilidades penales y las demás previstas por las leyes. 4. Los obligados por el deber de reserva no podrán prestar declaración ni publicar, comunicar o exhibir datos o documentos reservados, ni siquiera después de haber cesado en el servicio, salvo permiso expreso, según corresponda, del órgano competente de la Agencia Estatal de Seguridad Aérea o de la Comisión de Investigación de Accidentes e Incidentes de Aviación Civil, que sólo podrá otorgarse en los supuestos previstos en el artículo siguiente o en la normativa comunitaria que sea de aplicación. Si dicho permiso no fuera concedido, la persona afectada mantendrá la reserva y quedará exenta de la responsabilidad que pudiera derivarse de denegar información a las instancias indicadas en dicho precepto. 5. Los sujetos del sector público y privado obligados por el Programa Estatal de Seguridad Operacional para la Aviación Civil establecerán protocolos que permitan preservar el carácter reservado de la información...».

[24] Este proceso se está produciendo en todos los países de nuestro entorno, a modo de ejemplo, BSI (Bundesamt für Sicherheit in der Informationstechnik) es la agencia alemana responsable de la seguridad de la información. El BSI ha desarrollado directrices para el borrado de datos que se basan en las leyes alemanas, como la MIDA y la BDSG. Las directrices del BSI establecen que los datos personales deben ser eliminados de manera segura y completa. Esto significa que los datos deben ser irrecuperables. El BSI recomienda utilizar métodos de borrado seguros, como la eliminación física de los datos o la sobrescritura de los datos con datos aleatorios. Las directrices del BSI también establecen que los datos deben ser eliminados cuando ya no sean necesarios para el propósito para el que fueron recopilados. Esto significa que los datos deben ser eliminados regularmente, por ejemplo, cada año o cada dos años. Los proveedores de servicios de intermediación deben cumplir con las directrices del BSI para el borrado de datos. Si no lo hacen, pueden ser sancionados por el BSI.

[25] Implícitamente, la [STC 230/2007, de 5 de noviembre](#) establece que «...Por lo que se refiere al derecho al secreto de las comunicaciones ([art. 18.3 CE](#)), este Tribunal ha reiterado que este derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. El bien constitucionalmente protegido es así — a través de la imposición a todos del «secreto»— la libertad de las comunicaciones, por lo que dicho derecho puede resultar vulnerado tanto por la interceptación en sentido estricto —que suponga aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación— como por el simple conocimiento antijurídico de lo comunicado —apertura de la correspondencia ajena guardada por su destinatario, por ejemplo. Igualmente se ha destacado que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores, de ahí que se haya afirmado que la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del

---

teléfono, requiere resolución judicial, toda vez que el acceso y registro de los datos que figuran en dichos listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones (por todas, [SSTC 123/2002, de 20 de mayo](#), F. 4, ó [56/2003, de 24 de marzo](#), F. 2, y SSTEDH de 2 de agosto de 1984, caso Malone c. Reino Unido, § 84 y, entre las últimas, de 3 de abril de 2007, caso Copland c. Reino Unido, § 43)...»