# LA SEUDONIMIZACIÓN Y LA ANONIMIZACIÓN DE DATOS PERSONALES EN LAS SENTENCIAS DEL ORDEN JURISDICCIONAL SOCIAL*

**Yolanda Cano Galán****
Universidad Rey Juan Carlos

**SUMARIO:** –1. Introducción. –2. Marco normativo de la protección de datos en las sentencias. 2.1. Normativa europea. 2.1.1. Tratamiento de datos de carácter personal y derechos fundamentales. 2.1.2. El Reglamento General de Protección de Datos. 2.2. Normativa española. 2.2.1. El mandato constitucional de protección de datos de carácter personal y la Ley Orgánica de Protección de Datos Personales. 2.2.2. La Ley Orgánica del Poder Judicial. 2.2.3. La Ley Reguladora de la Jurisdicción Social y la Ley de Enjuiciamiento Civil. 2.2.4. El Reglamento del CGPJ 1/2005, de los aspectos accesorios de las actuaciones judiciales. –3. Precisiones terminológicas. 3.1. Definiciones. 3.1.1. Seudonimización. 3.1.2. Minimización de datos. 3.1.3. Cifrado de datos. 3.1.4. Anonimización. 3.1.5. Disociación de datos. 3.1.6. Supresión de datos. 3.2. Obligaciones vinculadas a las definiciones. 3.2.1. Obligaciones diferenciadas "ad intra" y "ad extra": ¿un camino hacia el absurdo? 3.2.2. "Anonimización" y "perjudicados": dos términos sin definición legal y un nuevo galimatías obligacional. 3.2.3. La solución: la "seudonimización" como regla general y la "anonimización" de datos de categoría especial con efectos "ad extra". –4. Datos personales susceptibles de seudonimización y anonimización. –5. Problemas prácticos de la seudonimización y la anonimización y sus soluciones. 5.1. Problemas derivados de la seudonimización y anonimización de datos personales contenidos en sentencias objeto de recurso. 5.1.1. La no seudonimización o anonimización de datos personales de las sentencias recurridas. 5.1.2. La seudonimización y anonimización de datos personales en sentencias invocadas de contraste en los recursos de casación para la unificación de doctrina. 5.2. Problemas derivados de la expedición de certificación literal de sentencias seudonimizadas o anonimizadas. 5.3. Problemas derivados de la seudonimización o anonimización de los nombres de los abogados. 5.4. Las soluciones. –6. Conclusiones.

RESUMEN

*El presente estudio examina las obligaciones contenidas en la normativa comunitaria y española para garantizar el derecho a la intimidad de las personas físicas mediante la seudonimización y anonimización de datos personales contenidos en las sentencias del orden jurisdiccional social. Se identifican y definen los términos seudonimización, minimización de datos, cifrado de datos, anonimización, disociación de datos, supresión de datos, y se examinan las obligaciones vinculadas a cada uno de dichos términos. El estudio, además, aborda problemas específicos sobre la forma en que se está llevando a cabo la seudonimización y anonimización de datos personales en las sentencias y avanza soluciones para garantizar los derechos vinculados a la protección de datos sin vulnerar el derecho a la tutela judicial efectiva.*

*ABSTRACT*

*This paper examines the obligations created by the UE and Spanish regulations protecting workers with regard to the processing of personal data in the text of the judgments handed down by judges and social courts. The terms pseudonymisation, minimization of personal data, encryption of personal data, anonymization, minimization of personal data, dissociation of personal data and deletion of personal data, are identified and defined in this paper, clarifying the obligations related to each of these terms. The paper addresses specific problems about how pseudonymisation and anonymization of personal data are being carried out in judgemens and offers solutions to guarantee the rights related to personal data protection without violating the right to obtain a fair judgment.*

**Palabras clave:** datos personales, seudonimización, anonimización, cifrado de datos personales, minimización de datos personales, disociación de datos personales, supresión de datos personales, sentencias, protección de datos personales, derecho a la intimidad de los trabajadores.

**Key words:** personal data, pseudonymisation, anonymization, encryption of personal data, minimization of personal data, dissociation of personal data, deletion of personal data, judgments, protection of personal data, right to privacy of workers.

## 1. INTRODUCCIÓN

¿Podría la trabajadora Ana María De Diego Porras reclamar derechos de autor o indemnizaciones por la identificación de sentencias con su nombre? En estos tiempos de gran preocupación por la protección de datos personales, especialmente en internet y en las redes sociales, no puede dejar de sorprender que muchas de las sentencias que han provocado una importante reacción social, cambios jurisprudenciales, impulsos de modificación normativa, y ríos de tinta, tanto en forma de artículos de prensa como doctrinales, se conozcan, precisamente, por el nombre de los trabajadores que impulsaron el proceso judicial correspondiente.

El nombre de las personas es el dato más personal que existe, por lo que el hecho de que haya resoluciones judiciales que se conozcan, precisamente, por dicho nombre, nos obliga a reflexionar cómo la utilización de datos personales en las sentencias puede afectar a derechos tan fundamentales como "el derecho al honor, a la intimidad personal y familiar y a la propia imagen" –art. 18.1 CE–. Dicho derecho, unido a la obligación contenida en el apartado 4 del propio precepto (art. 18 CE) –"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"– nos obliga a reflexionar sobre cómo se debe garantizar el derecho a la intimidad en el ámbito del proceso laboral[1].

* Recibido el 24 de febrero de 2020. Aceptado el 17 de abril de 2020.
** Letrada del Gabinete Técnico del Tribunal Supremo. Profesora Titular de Derecho de Trabajo y de la Seguridad Social.

[1] UTRILLA HERNÁN, R. "Acceso a los datos de los ficheros judiciales: especial referencia a los textos de las sentencias contenidas en dichos ficheros, derechos de rectificación por los interesados" *Estudios Jurídicos. Cuerpo de Secretarios Judiciales,* núm. 1, 2000, pág. 566, va más allá, y distingue el derecho al a intimidad del derecho al a privacidad, respecto del que entiende es *"un concepto más amplio que el anterior",* y que pueden *"resultar menoscabado por la indebida utilización de las actuales tecnologías informáticas".* Añade que *"se trata de proteger la privacidad pero también de buscar el equilibrio entre la libertad de expresión –que comprende la libertad de opinión y la libertad de comunicar o recibir informaciones– y la protección de la esfera privada de los individuos cuando se produce una intromisión en ella por el tratamiento de sus datos".* En parecidos términos se pronuncia GARCÍA HERRERA, V. "Transparencia jurisdiccional y protección de datos. La anonimización de sentencias", *Actualidad Civil*, núm. 3, 2019, si bien señala que las personas que no ostentan la condición de interesados *"tendrán acceso a las resoluciones judiciales a través del Portal del Poder Judicial, pero este acceso no lo será al texto íntegro de las mismas, sino que será restringido, dado que sólo podrán consultarse previo un proceso de anonimización, una vez han sido expurgados los nombres, direcciones y cualesquiera otros datos personales de las partes".*

[2] DO C 202/389, de 7 de junio de 2016.

[3] DO C83/49, de 30 de marzo de 2010.







El derecho a la intimidad de los trabajadores se puede abordar desde múltiples perspectivas jurídico-laborales: videovigilancia en el trabajo, control del uso del correo electrónico u otras tecnologías, el uso de algoritmos discriminatorios para la selección de personal, etc. Sin embargo, existe un aspecto poco examinado en la doctrina iuslaboralista con importantes consecuencias laborales: la necesidad de garantizar el derecho a la intimidad en las resoluciones judiciales, primordialmente las sentencias.

En el mundo de internet, de las bases de datos jurisprudenciales y de una prensa que publica la noticia antes incluso de que sea conocida por las partes de un proceso, el conocimiento de datos personales que suelen aparecen en las resoluciones judiciales puede provocar no pocas consecuencias negativas para las partes en conflicto. Por poner un ejemplo, una empresa puede indagar qué trabajadores tienen una alta conflictividad –información que podría obtenerse de las sentencias–, para no contratarles, o puede averiguar cuál había sido su salario anterior y cuándo fue despedido para minorar las condiciones retributivas de su oferta laboral. Por ello, parece conveniente examinar, de forma crítica, la forma en que se está garantizando el derecho a la intimidad a través del examen de lo que se conoce como anonimización y seudonimización de sentencias, indagando los problemas que plantea la falta de una regulación clara al respecto y de la compleja coordinación entre los mandatos contenidos en la normativa comunitaria y la española, y ello, fundamentalmente, en aras a garantizar los derechos fundamentales de los trabajadores.

## 2. MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS EN LAS SENTENCIAS

### 2.1. Normativa europea

#### *2.1.1. Tratamiento de datos de carácter personal y derechos fundamentales*

Ni la Carta de Derechos Fundamentales de la UE[2] ni el Tratado de Funcionamiento de la UE[3], contienen una previsión específica sobre la protección de datos personales en las resoluciones judiciales, sino que sólo contemplan aspectos genéricos de la protección de dichos datos personales en cuanto que garantía de los derechos fundamentales.

En particular, el art. 7 de la Carta de Derechos Fundamentales de la UE contempla que *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"*. Además, el art. 8.1 de la Carta de Derechos Fundamentales de la UE concreta que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*, abundando el apartado segundo en que *"estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley"*.

Por su parte, el art. 16.1 del Tratado de Funcionamiento de la Unión Europea, determina que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*, abundando el apartado segundo en que *"El parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión y sobre la libre circulación de estos datos"*.

Como se ha avanzado, todos estos estos preceptos vinculan la protección de datos personales a derechos fundamentales, en particular, el derecho a la intimidad de las personas –aunque también otros como el honor, la propia imagen, etc.[4]–, convirtiéndose la protección de datos en un derecho en sí mismo y en una obligación que deben cumplir quienes deban tratar dichos datos, cuestiones éstas no libres de problemas cuando de garantizar los mismos se trata en los procedimientos judiciales, y especialmente en las sentencias que se dicten, y ello aunque el Derecho originario de la Unión Europea (UE) no contemple previsión específica alguna al respecto.

#### *2.1.2. El Reglamento General de Protección de Datos*

Para garantizar los derechos fundamentales en juego, es preciso adoptar una legislación que regule cómo deben protegerse los datos personales, especialmente cuando éstos aparecen en sentencia. La primera aproximación a cómo debe realizarse la protección en el marco de procedimientos judiciales, se contiene en 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[5] (en adelante Reglamento General de Protección de Datos o RGPD[6]), ya que el Reglamento (UE) 2018/1725[7] sólo afectará al tratamiento de datos por instituciones, órganos y organismos de la Unión, y no tiene relevancia respecto de la cuestión aquí analizada[8].

No nos puede sorprender –dada la escasa importancia que se da a la cuestión relativa a la protección de datos en las sentencias en perspectiva comunitaria–, que el RGPD no contemple de forma expresa o directamente la cuestión que estamos examinando. Sin embargo, el marco de derechos y obligaciones que construye, puede servir de guía para el análisis de cómo tienen que garantizarse la protección de datos personales en las sentencias.

Del RGPD debe destacarse que el mismo se aplica, únicamente, al tratamiento de datos personales de las personas físicas, sin que incluya a las *"personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto"* –considerando 14–, y ello teniendo en cuenta que su finalidad es *"establecer las normas relativas a la protección de las personas físicas en lo que respecta al*

[4] Vid. MARTÍNEZ MOYA, J. "La protección de datos en el derecho orgánico judicial", CGPJ, 2018, que determina que el derecho a la protección de datos nace *"de la necesidad de proteger la dignidad y de aquellos derechos personalísimos vinculados a la misma"*.

[5] Por el que se deroga la Directiva 95/45/CE.

[6] Que entró en vigor el 25 de mayo de 2018.

[7] Del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

[8] El Reglamento establece *"las normas relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por las instituciones y organismos de la Unión y las normas relativa a la libre circulación de dichos datos entre ellos o entre ellos y destinatarios establecidos en la Unión"* –art. 1.1–. Respecto de la cuestión que estamos examinando, sólo se contiene una previsión, en el art. 49, en orden a que *"cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional"*.

*tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos"* –art. 1 RGPD–. La conclusión es clara, la protección de datos sólo se garantiza respecto de las personas físicas, lo que, trasladado al marco de relaciones laborales, podría alcanzar: a los trabajadores asalariados o autónomos, a los funcionarios, a los cooperativistas de trabajo asociado y a los empresarios que sean personas físicas. El considerando 14 no lo aclara, ni el articulado del RGPD tampoco –al referir únicamente a personas jurídicas–, pero del mismo podría deducirse que las garantías contempladas en el RGPD no alcanzarían a las empresas, sea cual sea la forma de constitución de las mismas, ni a las fundaciones, asociaciones, y cualesquiera otras que no puedan ser consideradas como personas físicas, a pesar de que los responsables de las mismas sí lo sean.

Además, el RGPD, en su considerando 20, concreta que el mismo afecta *"a las actividades de los tribunales y otras autoridades judiciales"* con el matiz de que *"A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial"*[9]. Parece claro, aunque no se contemple en el articulado del RGPD, que las garantías establecidas en relación con la protección de datos de las personas físicas, alcanzará a las sentencias, y ello por cuanto las mismas no suponen más que una de la "actividades de los tribunales" a las que refiere. Un avance de conclusiones: la protección de dichos datos alcanzará al conocimiento público de las sentencias, más no a efectos del ejercicio de la *"función judicial"*, cuestión ésta sobre la que se reflexionará con mayor detenimiento posteriormente.

Dada la escasa importancia que se da a la cuestión ahora analizada en el RGPD, no puede sorprender el hecho de que tampoco se aclare cómo debería hacerse efectiva la garantía en el ámbito judicial en general, y en particular respecto de las sentencias. Lo que sí parece claro es que en dicho ámbito debe ser de aplicación lo dispuesto en el art. 25.1 RGPD, en que se contempla, respecto de los responsables del tratamiento, que *"aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebida para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos"*.

Conforme a dicho precepto, y poniendo en relación el mismo con lo dispuesto en el considerando 20 RGPD –que extendía las obligaciones contempladas en el RGPD a las sentencias– parece claro que las sentencias deberán ser objeto de seudonimización, término definido en el art. 4.5) RGP como *"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"*.

La aparente claridad del precepto se oscurece cuando el art. 32 RGPD, al examinar la seguridad del tratamiento, incluye *"la seudonimización y el cifrado de datos personales"*. La conjunción "y" utilizada en el precepto, nos lleva a plantearnos si además de la seudonimización es preciso realizar alguna labor adicional como el *"cifrado de datos"*, o por el contrario el mismo no supone más que una de las formas para llevar a cabo la seudonimización. Dado que posteriormente se realizarán precisiones terminológicas sobre cómo debe garantizarse la protección de datos en las sentencias, abundaremos en este problema más adelante.

[9] Puesto que el considerando 20 del RGPD también determina que *"el tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular (…) concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este"*, es por lo que ha parecido conveniente, en cumplimiento de dicho considerando, examinar la cuestión abordada en el presente estudio.





La situación se complica aun más, cuando el considerando 26 RGPD alude a que *"el presente Reglamento no afecta al tratamiento de (…) información anónima"*, que se identifica en dicho considerando como la *"información que no guarda relación con una persona física identificada o identificable"*, añadiendo la referencia a *"datos convertidos en anónimos"*, respecto de los que refiere que *"el interesado no sea identificable o deje de serlo"*. Si bien parece claro que el RGPD estaría eliminando la "anonimización" de las obligaciones que contempla, podría sorprender que cuando de sentencias se habla, en España se utilice el término *"anonimización"*, confusión provocada por la falta de claridad terminológica respecto de las obligaciones que rodea a la protección de datos personales contenidos en las sentencias, y que exige una meditada reflexión que se abordará posteriormente.

**2.2. Normativa española**

*2.2.1. El mandato constitucional de protección de datos de carácter personal y la Ley Orgánica de Protección de Datos Personales*

En cumplimiento del mandato del art. 18.4 CE –*"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*–, España fue pionera en la adopción de normativa en materia de protección de datos[10], pero es como consecuencia de la aprobación del RGPD cuando se exige *"la elaboración de una ley orgánica que sustituya la actual"*[11], para adaptar el ordenamiento jurídico español al RGPD.

Dicha norma es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDP), que no refiere, expresamente, a la necesidad de seudonimización –en términos del RGPDP– de las resoluciones judiciales u otros datos necesarios para el ejercicio de la función jurisdiccional, simplemente señalándose, en el art. 77. 1 b), y en relación con el "Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento", que dicho régimen "será de aplicación a los tratamientos de los que sean responsables o encargados (…) b) los órganos jurisdiccionales".

En conclusión, ni la LOPDP ni el RGPD refieren expresamente a las sentencias, pero ello no implica que no exista la obligación de proteger datos de carácter personal en todas y cada una de las que se dicten; al contrario, sobre las mismas se proyectan todas las obligaciones del RGPD y de la LOPDP, aunque no se contemple la obligación expresamente.

*2.2.2. La Ley Orgánica del Poder Judicial*

Es en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante LOPJ) donde se contemplan las referencias expresas a la cuestión que estamos examinando, en particular, en el capítulo I bis –*"Protección de datos de carácter personal en el ámbito de la Administración de Justicia"*[12]–, arts. 235 bis y 236 bis a decies. Antes de examinar las obligaciones establecidas en la LOPJ, es preciso realizar una precisión previa. Los art. 235 bis y 236 bis a decies siguen refiriendo a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[13], respecto de la que, de conformidad con lo dispuesto en la DA 14ª LOPDP, sólo siguen en vigor los arts. 23 y 24, y la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiesen entrado en vigor con anterioridad a la fecha de aplicación del RGPD *"en tanto no sean expresamente modificadas, sustituidas o derogadas"*[14]. En consecuencia, cuando la LOPJ refiera a dicha norma, en realidad la referencia debería entenderse hecha a la LOPDP.

[11] Exposición de motivos de la LOPDP.

[12] Añadido por el art. Único 36 de la Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, para *"intensificar la protección de los derechos (…) como es la protección de datos en el ámbito de los Tribunales, que carecía hasta hoy de una regulación completa y actualizada"*, conforme a su Exposición de Motivos.

[13] Adoptada para trasponer al ordenamiento jurídico español la Directiva 94/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1994, 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, derogada por el RGPD. La referencia que se contiene en la norma, debería entenderse hecha a la Ley orgánica 3/1028 de 5 de diciembre de Protección de Datos personales.





Conforme al art. 236 bis LOPJ, los jueces y tribunales deben cumplir con las obligaciones de tratamiento de datos contempladas en el RGPD y en la LOPDP, y ello *"con ocasión de la tramitación por los Tribunales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial"*. El precepto hace expansiva la obligación de tratamiento de datos, y ello por cuanto extiende dicha obligación no sólo en el marco del proceso que se esté desarrollando, sino también en las actuaciones de la oficina judicial, lo que supone que tanto los Jueces, los Letrados de la Administración de Justicia y los funcionarios que trabajan en las unidades procesales de apoyo directo o en los servicios comunes procesales, deberán cumplir con los mandatos del RGPDP y de la LOPDP, no sólo respecto de las sentencias, sino también respecto de cualquier otro tipo de resolución o acto de comunicación –providencias, diligencias de ordenación, oficios, etc. Dicha obligación, que no pocos problemas ocasiona, sin embargo excede el ámbito de este estudio, por lo que sirva una simple mención a la misma.

Debe recordarse que la LOPJ no contempla la obligación de anonimización o seudonimización de sentencias u otros documentos necesarios para el desarrollo del proceso o para el ejercicio de la función jurisdiccional, por lo que puede plantearse la cuestión de si existiría la obligación de articular algún mecanismo de protección del tratamiento de datos en las sentencias y en caso de respuesta positiva, cuál debería ser éste.

La respuesta tiene que ser necesariamente positiva. Es el art. 235 bis LOPJ el que clarifica la cuestión. El precepto concreta la obligación en los siguientes términos: *"Sin perjuicio de lo establecido en el párrafo segundo del apartado 1 del artículo 236 quinquies y de las demás restricciones que, en su caso, pudieran establecerse en las leyes procesales, el acceso al texto de las sentencias, o a determinados extremos de las mismas, o a otras resoluciones dictadas en el seno del proceso, sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda"*.

Puesto que el precepto remite al art. 236 quinquies LOPJ, parece conveniente examinar la obligación que establece dicho precepto. En el mismo se concreta que *"Los Jueces y Tribunales, y los Letrados de la Administración de Justicia conforme a sus competencias procesales, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar su derecho a la tutela judicial efectiva"*, añadiendo que *"Del mismo modo procederán respecto del acceso por las partes a los datos personales que pudieran contener las sentencias y demás resoluciones dictadas en el seno del proceso"*[15].

[14] En particular, la DA 14, concreta que *"las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1994, 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, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018 (…) siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas"*.

[15] El precepto amplía la obligación no sólo a las sentencias, sino también a cualquier otro dato personal que haya surgido en el marco del proceso, y ello cuando el art. 236 quinquies 2 LOPJ determina que *"En todo caso será de aplicación lo dispuesto en la legislación de protección de datos de carácter personal al tratamiento que las partes lleven a cabo de los datos que les hubieran sido revelados en el desarrollo del proceso"*.





La coordinación de ambos preceptos parece complicada, y ello por cuanto ambos instituyen la obligación de garantía del derecho a la protección de datos de carácter personal en las sentencias, si bien aludiendo a términos no contemplados en el RGPD –el RGPD refería a la "seudonimización" y "cifrado de datos", mientras que la LOPJ refiere a "disociación de datos", "supresión de los datos personales"–, lo que podría hacer pensar que la forma de garantizar el derecho en el ordenamiento jurídico español no es plenamente coincidente con el comunitario, lo que, como después se profundizará, no es completamente cierto. Existe igualmente complejidad respecto de si la forma de garantía es diferenciada o no, pero ésta, igualmente, es una cuestión sobre la que se profundizará posteriormente.

*2.2.3. La Ley Reguladora de la Jurisdicción Social y la Ley de Enjuiciamiento Civil*

La Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (en adelante LRJS), no contiene referencia alguna a la cuestión que estamos examinando. Sí, por el contrario, aparece una previsión en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante LEC), de aplicación supletoria en el ámbito laboral conforme a lo dispuesto en la DA 4ª LRJS[16].

El art. 212.2 LEC, en la línea de lo dispuesto en los artes. 235 bis y art. 236 quinquies LOPJ, concreta que *"se permitirá a cualquier interesado el acceso al texto de las sentencias o a determinados extremos de las mismas. Este acceso sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contribuyeran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requiera un especial deber de tutela, a la garantía del anonimato de los perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contradictorios a las leyes"*.

Las obligaciones que contempla no son exactamente coincidentes ni con lo dispuesto en el RGPD –que alude a *"seudonimización"* y *"minimización"* y *"cifrado"*–, ni con el texto de los art. 235 bis LOPJ y 236 quiquies LOPJ, –que aluden a la *"disociación de datos"* y *"supresión de los datos personales"*–, ya que refiere, en el mismo párrafo, a la *"disociación"* –término éste sí coincidente con el del art. 235 bis LOPJ–, y al *"anonimato de los perjudicados"*, de lo que debe plantearse si éstos son términos distintos a los utilizados por el RGPD o tienen algún tipo de vinculación con los allí manejados, planteando igualmente problemas respecto de a qué mecanismos de los allí identificados se debe recurrir para garantizar el derecho a la intimidad en las sentencias, cuestión ésta, nuevamente, que será objeto de tratamiento pormenorizado posteriormente.

*2.2.4. El Reglamento del CGPJ 1/2005, de los aspectos accesorios de las actuaciones judiciales*

Por mandato del art. 230.5 LOPJ –en redacción dada por la LO 16/1994, de 8 de noviembre–, el Consejo General del Poder Judicial (en adelante CGPJ) tiene la competencia para determinar reglamentariamente los requisitos y condiciones que afecten al establecimiento y gestión de los ficheros automatizados que estén bajo la responsabilidad de los órganos judiciales, a fin de que se asegure la observancia de las garantías y derechos establecidos en la Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal, referencia que hoy ha de entenderse hecha a la LOPDP.

Para cumplir dicho mandato, por Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial, se aprobó el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales, en que se contienen importantes previsiones respecto de la cuestión que estamos analizando. En particular, el art. 3.2, tras establecer en el apartado primero

[16] Que concreta que *"En lo no previsto en esta Ley regirá como supletoria la Ley de Enjuiciamiento Civil"*.

que *"los interesados podrán acceder al texto de la sentencias"*, concreta que *"se podrá restringir el acceso al texto de las sentencias o a determinados extremos de las mismas, cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas dignos de especial tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, y, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes"*, estableciendo el art. 4 que *"Corresponde a los Secretarios de la Oficina judicial facilitar a los interesados el acceso a los documentos judiciales a que se refieren los dos artículos anteriores"*.

El Reglamento no utiliza ninguno de los términos hasta ahora avanzados, sino que simplemente establece una especie de prohibición –*"restringir el acceso"*– cuando pudiera afectar a la intimidad de personas necesitadas de especial tutela –sin definir cuáles son éstas–, e imponiendo una obligación aún más restrictiva cuando refiere a que las sentencias deberán garantizar el *"anonimato de víctimas o perjudicados"* –nuevamente sin definir quiénes pueden ser éstos–.

A los problemas terminológicos que se proyectan sobre la garantía de la protección de datos personales en las sentencias, derivados de la diferente terminología que se utiliza en el RGPDP, LOPDP, LOPJ y LEC, el Reglamento viene a plantear un problema terminológico adicional, y ello por cuanto incorpora un segundo nivel de coordinación de cómo se tengan que proteger los datos, al distinguir entre "personas necesitadas de especial tutela" –respecto de las que se podrá restringir el acceso a las sentencias– y *"víctimas o perjudicados"* –respecto de las que se deberá garantizar el anonimato. La solución no es sencilla, y como se ha avanzado, la respuesta sólo puede ir de la mano de la comprensión de qué obligaciones se establecen realmente en las normas analizadas –seudonimización, anonimización, cifrado de datos, supresión de datos, etc.–, ya que sólo entonces se podrá dilucidar el nivel de la obligación respecto de los colectivos mencionados.

## 3. PRECISIONES TERMINOLÓGICAS

De lo hasta ahora expuesto se deduce que el problema que presenta actualmente la regulación de la protección de datos en las sentencias, es, fundamentalmente, terminológico, y ello por cuanto sólo se podrá examinar el fondo de la cuestión que estamos examinando previa identificación de las obligaciones contempladas en las normas, que, como se ha visto, no son uniformes terminológicamente.

Como se avanzó, el RGPD refería a cuatro conceptos: *"seudonimización"*, *"minimización de datos"* [17], *"cifrado de datos personales"* [18] y *"anonimización"* [19]. Por su parte, el art. 235 bis LOPJ aludía a la *"disociación de los datos de carácter personal"*, en "el acceso al texto de las sentencias, o a determinados extremos de las mismas" –en parecidos términos se pronunciaba el art. 212.2 LEC–, mientras que el art. 236 quinquies 1 LOPJ, aludía a la obligación de *"supresión de los datos personales que pudieran contener las sentencias y demás resoluciones dictadas en el seno del proceso"*.

[17] Art. 25.1 RGPD cuando estableció la obligación de establecer *"medidas técnicas y organizativas apropiadas, como la seudonimización, concebida para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos"*.

[18] Art. 32 RGPD, que al examinar la seguridad del tratamiento, refería a *"la seudonimización y el cifrado de datos personales"*.

[19] Considerando 26 RGPS, cuando determina que *"los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo"*.





El primer problema a examinar es si cada término se identifica con una obligación diferenciada, o por el contrario todos o algunos de ellos podrían considerarse coincidentes[20], en cuyo caso se haría preciso: 1) Definir éstos; 2) Concretar las obligaciones que se derivan de cada definición; y 3) Examinar a qué información corresponde cada una de las obligaciones.

### 3.1. Definiciones

#### *3.1.1. Seudonimización*

El RGPD sólo define uno de los términos que del examen conjunto de la normativa se podrían identificar con obligaciones respecto de la protección de datos personales en las sentencias. Éste es el término *"seudonimización"*, entendido como *"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"* –art. 4.5) RGPD.

De un análisis de la definición se puede concluir que la seudonimización sería una especie de *"borrado"* de datos personales, es decir, referiría a la aplicación de técnicas que imposibilitaran la identificación de la persona física, de forma que, a simple vista, o sin realización de operaciones complejas, no podría llegarse a conocer quién es ésta o sus datos personales[21]. El avance de la técnica permite, ya, de forma sencilla, realizar dicha operación, ya que simplemente implicaría sustituir el dato a seudonimizar por otro que nada tenga que ver con éste, si bien sería posible, de conocer qué dato personal se ha sustituido por otro, a qué dato en particular refiere –por cuanto el anterior se tendría que mantener en ficheros separados–, y si bien sería igualmente posible, por el avance de la técnica y fundamentalmente a través de operaciones de big data, llegar a conocer cuál es el dato personal no seudonimizado[22]. Pongamos un ejemplo. Parece claro que el dato más personal que existe es el nombre de las personas –así comenzábamos este estudio–, por lo que si tuviéramos que seudonimizar el mismo, sería posible, por ejemplo, sustituir el nombre verdadero por otro imaginario o aleatorio. De esta forma no sería posible identificar a la persona a la que refiere, pero a través de operaciones complejas –algoritmos que conectaran otros datos referidos a la persona no susceptibles de seudonimización con el big data, por ejemplo–, podría identificarse quién es ésta, e igualmente el Letrado de la Administración de Justicia –en cuanto que responsable de seguridad y del tratamiento de datos a los efectos previstos en la legislación de protección de datos de carácter personal conforme al art. 236 sexies 3 LOPJ–, podría identificar el nombre de la persona por cuanto el mismo debería contenerse en un fichero independiente.

[20] NIETO MANIBARDO, E. "Anonimización, seudonimización y disociación" en *Fodertics 7.0*: estudios sobre derecho digital. GONZÁLEZ PULIDO, I. – BUENO DE MATA, F. (Coords.), pág. 148, llega a afirmar que *"la forma en que el legislador utiliza los términos "disociación", "anonimización" y "seudonimización" es incoherente (…) nuestra legislación es contradictoria e incongruente al utilizar dicha terminología y, en mi opinión, no quedan claro lo que debe entenderse por cada uno de tales conceptos"*.

[21] MIRALLES LÓPEZ, R.M. "Desvinculando datos personales: seudonimización, desindentificación y anonimización", *I+S: Revista de la Sociedad Española de Informática y Salud*, núm. 122, 2017, pág. 8 identifica el término como *"eliminar de un conjunto de datos personales la vinculación con la persona, manteniendo separadamente la información necesaria para volver a vincular la información (re-identificar)"*.

[22] NIETO MANIBARDO, E. "Anonimización…", *op. cit.* pág. 142, alude a información reversible o irreversible, señalando que *"existen datos personales eliminados de un conjunto de datos que no permitan identificar a una persona, pero la hacen potencialmente identificable, bien porque hay información adicional que se encuentra separada o bien porque la información adicional está en otras fuentes. Se trata de aquella información reversible, por contraposición a la irreversible, que es aquella que no puede identificar a la persona, y además tampoco se va a poder reidentificar usando otras fuentes"*.





#### *3.1.2. Minimización de datos*

El RGPD, a pesar de aludir a *"minimización de datos"*, no define, a diferencia de la seudonimización, dicho concepto. Conforme a la definición realizada por la Real Academia Española (RAE), minimizar consistiría en *"reducir lo más posible el tamaño de algo o quitarle importancia"*. Conjugando dicha definición con la definición de seudonimización contemplada en el RGPD, podríamos considerar que ambos términos no son coincidentes, ya que una cosa es no poder atribuir un dato a un interesado sin utilizar información adicional –en términos de la definición de seudonimización del RGPD– y otra reducir dicho dato o quitarle importancia –en términos de la definición de la RAE. Sin embargo, nada obsta para que ambos puedan considerarse esencialmente sinónimos, y ello por cuanto en ambas definiciones se contempla una especie de obligación de sustitución de un dato por otro; obligación, eso sí, de mayor calado en el supuesto de la seudonimización que en el de la minimización, y ello como consecuencia de que la diferencia podría estar en la forma en que dicha sustitución o borrado de dato se realice. Siguiendo con el ejemplo anterior. Un dato se seudonimizaría si se sustituyera el nombre y apellidos por otro imaginario o aleatorio, pero se minimizaría si simplemente se pusieran las iniciales. En el primer supuesto sería difícil –salvo la realización de labores complejas de la que antes hemos dado algún ejemplo– conocer el nombre y apellidos verdaderos de la persona. En el segundo, sin embargo, por las simples iniciales, podría identificarse ésta por personas allegadas o por el público en general si la persona es, por ejemplo, conocida. Es por ello, por lo tanto, y por lo que como se avanzó, la minimización, si bien podría quedar encuadrada en la definición de seudonimización, supone un estadio menor de protección que ésta.

#### *3.1.3. Cifrado de datos*

Tampoco define el RGPD el concepto *"cifrado de datos"* a pesar de referir al mismo en el art. 32 RGPD. Recurriendo nuevamente a la definición de la RAE, *"cifrado"* es *"escrito en cifra"*. De dicha definición se deduce que en realidad no se trataría de un concepto diferenciado de la seudonimización, ya que si ésta supone una garantía de que los datos personales no se atribuyen a una persona física identificada o identificable, el cifrado de datos no supondría más que una forma de evitar que dicha atribución se produzca, y ello a través, precisamente, de la sustitución del dato correspondiente por una cifra. Tampoco supondría un concepto diferenciado del de minimización, ya que si éste se ha identificado con la reducción del dato, parece claro que dicha reducción podría realizarse a través del cifrado. El Diccionario de la RAE nos aclara la cuestión, ya que si bien en su acepción primera define *"cifra"* como un *"número dígito"*, en su acepción tercera la identifica con la *"escritura en que se usan signos, guarimos o letras convencionales, y que solo puede comprenderse conociendo la clave*", término éste fácilmente identificable con el de *"seudonimización"* definido en el RGPD. Además, en su acepción tercera, la RAE identifica el término *"cifra"* con el *"enlace de dos o más letras, generalmente las iniciales de nombres y apellidos, que como abreviatura se emplea en sellos, marcas, etc."*, definición ésta esencialmente coincidente con la de *"minimización"* en los términos examinados anteriormente.

#### *3.1.4. Anonimización*

Como se avanzó, el RGPD aludía a lo que aquí identificamos como *"anonimización"* en el considerando 26, y ello para aclarar que las obligaciones de protección de datos no alcanzan a la información anónima. Por su parte, el art. 212.2 LEC aludía a la *"garantía del anononimato de los perjudicados"*, y ello al referir a que el acceso a las sentencias se debería realizar previa disociación de datos de carácter personal, y nuevamente sin concretar cómo debe garantizarse ello.

La realidad es que siempre que se habla de la protección de datos en las resoluciones judiciales, y especialmente en las sentencias, sin embargo, se alude a que la información debe ser anónima, pudiendo cuestionarnos si la anonimización –término utilizado coloquialmente– refiere a la seudonimización, a la minimización o al cifrado de datos –términos utilizados legalmente, al menos en el RGPD.





Aunque ni el RGPD, ni la LOPD, ni la LOPJ, ni la LRJS, ni la LEC, definen *"anonimización"*, del contenido del considerando 26 del RGPD se puede elaborar una definición. En particular, cuando el considerando 26 RGPD alude a que *"los principios de protección de datos no deben aplicarse a la información anónima"*, aclara que la misma es "información que no guarda relación con una persona física identificada o identificable" y añade que tampoco se aplicará *"a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo"*. Por su parte, el Diccionario de la RAE define *"anonimizar"* como *"expresar un dato relativo a entidades o personas, eliminado la referencia a su identidad"*.

De la aclaración contemplada en el considerando 26 RGPD, y de la definición del Diccionario de la RAE, se puede deducir que la anonimización impediría totalmente la identificación de la persona física o de sus datos personales, bien porque la información nada tiene que ver con dicha persona física, bien porque se ha recurrido a complejas operaciones –generalmente informáticas– para eliminar cualquier dato que permitiera llegar a conocer a qué personas refiere o cuáles son sus datos personales[23]. Siguiendo con el ejemplo hasta ahora utilizado, si se quisiera anonimizar el nombre y apellidos de una persona en sentencia, ya no sería suficiente que se sustituyera el mismo por otro –*"seudonimización"*–, o que se cambiara por iniciales –*"minimización"*–, o que se sustituyera por cifras –*"cifrado de datos"*–, sino que simplemente se eliminaría dicho dato, y además no podría existir fichero separado que permitiera cumplimentar dicho vacío de dato con el nombre y apellidos verdadero de la persona. Si la obligación de anonimización existe respecto de los datos personales contenidos en la sentencia, debe ser objeto de análisis detenido y pormenorizado posteriormente.

#### *3.1.5. Disociación de datos*

El art. 235 bis LOPJ incorporaba un nuevo término en relación con las obligaciones de garantía de la protección de datos en las sentencias*: "disociación de datos"*, nuevamente, sin definir éste[24]. Y en idénticos términos se pronunciaba el art. 212.2 LEC, igualmente sin definir éste. Recurriendo a la definición de *"disociar"* contenida en el Diccionario de la RAE, ello supone *"separar algo de otra cosa a la que estaba unida"*, lo que, aplicado a los datos personales, supondría separar el dato personal de la persona física a la que se une el mismo. Dicha operación puede realizarse de diversas maneras, pudiendo ser éstas coincidentes con la disociación, la minimización, el cifrado de datos, e incluso con la anonimización, ya que todos estos términos también llevaban implícita dicha separación del dato personal de la persona a la que se une el mismo. Ello nos lleva a preguntarnos con cuál de dichos términos podría equipararse la *"disociación"*, e incluso si refiere a todos ellos, pero es ésta una cuestión que se abordará posteriormente, avanzándose que el mismo está vinculado a la seudonimización más no a la anonimización.

[23] MIRALLES LÓPEZ, R.M. "Desvinculando datos personales: seudonimización, desindentificación y anonimización", *I+S: Revista de la Sociedad Española de Informática y Salud*, núm. 122, 2017, pág. 9, identifica la anonimiación como una labor en la que *"se aplican operaciones adicionales sobre los datos ya desvinculados, de manera que no se pueda producir la re-identificación en base a otras fuentes de información (aquí se aplicarían funciones criptográficas, perturbación de datos, reducción de datos, etc."*. Por su parte, NIETO MANIBARDO, E. "Anonimización…", op. cit. pág. 143, aclara que el mismo se introduce en la legislación española en la Ley 14/2007, de 3 de julio, de Investigación biomédica, identificando el mismo como *"proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere"*.

[24] NIETO MANIBARDO, E. "Anonimización…", *op. cit.* pág. 143, señala que es *"el término clásico que venía utilizando el legislador, antes del surgimiento y desarrollo de la economía digital"*. Define el mismo, en relación con las sentencias, en relación a que *"se elimina toda referencia a las personas afectadas para proteger sus derechos de la privacidad"*.

*3.1.6. Supresión de datos*

Para terminar con el análisis de las definiciones de los conceptos vinculados a la protección de datos personales en las sentencias, y contemplados en las distintas normas que regulan la cuestión, debe analizarse qué debe entenderse por *"supresión de datos"*, término a que refiere el art. 236 quinquies 1 LOPJ. El mismo, como viene siendo habitual, no aparece definido en la norma, definiéndose en el Diccionario de la RAE el verbo "suprimir" –puesto que la "supresión" es *"la acción y efecto de suprimir"*–, como *"hacer desaparecer"* –acepción primera– u *"omitir"* –acepción segunda.

Siendo ello así, lo que parece claro es que la supresión no supondría una sustitución de un dato personal en términos de seudonimizacion, minimización, cifrado o disociación, sino que supondría una eliminación del dato, lo que concuerda, más bien, con el término anonimización anteriormente identificado y definido.

**3.2. Obligaciones vinculadas a las definiciones**

*3.2.1. Obligaciones diferenciadas "ad intra" y "ad extra": ¿un camino hacia el absurdo?*

Siguiendo con el esquema de razonamiento avanzado en el presente estudio, una vez definido cada término identificado en las normas reguladoras de la protección de datos personales en las sentencias, es preciso concretar si los mismos contienen obligaciones diferenciadas, y en caso afirmativo, respecto de qué datos personales.

Examinando las definiciones, parece claro que todas ellas pivotan sobre dos conceptos: seudonimización y anonimización. El primero aparece claramente como obligación en el RGPD, ya que el mismo no sólo lo define, sino que además concreta que la seudonimización forma parte de las obligaciones en relación al tratamiento de los datos personales, incluida la libre circulación de tales datos –art. 1 RGPD. Cómo deba realizarse la misma no aparece contemplado en norma alguna, si bien ésta podría llevarse a cabo a través de la minimización o cifrado de datos –en términos del RGPD– o a través de la disociación de datos –en términos de la LOPJ–. Así, seudonimizar supondría cambiar el dato personal por otro inventado, por iniciales –minimización–, o por cifras –cifrado– conforme al RGPD, incluyendo igualmente la disociación del dato a que refiere la LOPJ y la LEC, eso sí, sin eliminarlo, ya que debería mantenerse dicho dato en fichero separado, pudiendo ser éste encriptado pero en cualquier caso existiendo la posibilidad final –cuando se realicen operaciones complejas– de conocer la persona a la que refiere dicho dato.

Por su parte, la anomimización, que no aparece definida aunque sí mencionada en el RGPD y en la LEC, se identificaría con el concepto de supresión a que refiere igualmente el art. 212.2 LEC–, y supondría eliminar completamente un dato personal, de forma que ni siquiera recurriendo a operaciones complejas, pudiera llegar a conocerse el dato real o identificar la persona a la que refiere éste.

El porqué de la vinculación de cinco términos diferenciados a solo dos, debe resolverse no sólo examinando las similitudes respecto de la forma de tratamiento de datos que se extrae de las diferentes definiciones, sino sobre todo, de las obligaciones que se establecen en las normas –especialmente en la LOPJ y LEC– respecto del tratamiento de datos personales en las sentencias.

Profundicemos en el problema. Como se avanzó, el art. 235 bis LOPJ, refería a la "disociación de los datos de carácter personal" en *"el acceso al texto de las sentencias, o a determinados extremos de las mismas"*. Por su parte, el art. 236 quinquies 1 LOPJ, alude a la obligación de *"supresión de los datos personales que pudieran contener las sentencias y demás resoluciones dictadas en el seno del proceso"*.





El primero –art. 235 bis LOPJ–, refiere al *"acceso a las sentencias"*, vinculando a dicha acción una obligación, la de "disociación" de datos. El segundo –art. 236 bis LOPJ– refiere al "seno del proceso", vinculando dicho contexto a la "supresión" de datos personales. Puesto que como se ha avanzado los términos disociación y supresión no son términos coincidentes, ya que el primero se vinculaba a la seudonimización y el segundo a la anonimización, podría entenderse que lo que la LOPJ exige es seudonimizar los datos personales de las sentencias cuando se vaya a acceder a su texto fuera del proceso, mientras que se exigiría anonimizar los datos personales de las sentencias cuando se fuera a acceder a su texto en el seno del proceso. Dicho de otro modo, se impondría la obligación de seudonimizar, eso sí, *ad extra*, es decir, para partes ajenas al proceso –por ejemplo, consulta de sentencias por abogados ajenos al procedimiento, Jueces y Magistrados, académicos, prensa, público en general o incluso terceros interesados pero ajenos al proceso[25]–, mientras que se impondría la obligación de minimizar solamente *ad intra*, es decir, en el seno del proceso[26] –respecto de las partes del proceso, incluyendo los órganos jurisdiccionales encargados de enjuiciar la cuestión o resolver los recursos que se presenten frente a sentencias dictadas.

Si a ello añadimos que anonimizar supone un plus de garantía de la protección de datos –puesto que ni siquiera a través de operaciones complejas se podría llegar a identificar el dato y vincularlo a una persona física– respecto de la seudonimización –en que sí se podría identificar el dato e incluso vincularlo a la persona física mediante la realización de operaciones complejas–, parece un contrasentido que se establezca una mayor obligación cuando el acceso al texto de las sentencias se realiza por un tercero, que cuando se realiza por los propios órganos jurisdiccionales, ya que ¿cómo es posible que un tercero pudiera llegar a conocer del dato personal recurriendo a operaciones complejas, mientras que una parte del proceso no podría llegar a conocer de ninguna manera de un dato que pudiera ser crucial para la resolución de una controversia que le afecta y respecto de la que incluso podría ser condenado?

Dicha conclusión conduce al absurdo, ya que no se entendería el establecimiento de una obligación de mayor calado (anonimización), para garantizar la protección de datos en las sentencias que vayan a ser utilizadas por las partes del proceso (p. ej. a efectos de articular un recurso contra las mismas), mientras que se establecería una obligación de menor calado (seudonimización), respecto de partes ajenas al mismo y que necesitarían acceder al texto de las sentencias, no en funciones de defensa de los derechos de los trabajadores, sino de simple conocimiento, estudio o investigación.

La conclusión más acertada nos la ofrece la interpretación sistemática de las normas en que se establecen las obligaciones de seudonimización y anonimización. Recuérdese que el RGPD identificaba el término anonimización, pero para excluirlo del ámbito de protección del RGPD –ya que el considerando 26 RGPD aludía a que *"los principios de protección de datos no deben aplicarse a la información anónima"*–, mientras que el art. 212.2 LEC refería a la *"garantía del anonimato de los perjudicados"*. Puesto que el RGPD no establece obligación alguna respecto de la anonimización, y la misma sólo se contempla en el art. 212.2 LEC respecto de lo que considera *"perjudicados"*, la solución más adecuada al galimatías que provocaban los arts. 235 bis y 236 bis LOPJ, es que la seudonimización es la regla general, mientras que la anonimización sólo referiría a datos personales de quienes puedan quedar encuadrados en la categoría de *"perjudicados"*, eliminando de este modo el absurdo obstáculo de que existiera una obligación

[25] UTRILLA HERNÁN, R. "Acceso a los datos…", *op. cit.* pág. 582, identifica el término con terceros, que identifica con *"toda persona física o jurídica ajena al dato personal"*.

[26] UTRILLA HERNÁN, R. "Acceso a los datos…", *op. cit.* pág. 582, identifica el término con "interesado", entendiendo por tal *"persona directamente concernida por la información, denunciante, denunciado, inculpado, parte procesal, responsable civil, etc."*, abundando en que *"cuando la información sea requerida por una persona que tenga la cualidad de tercero, deberá contar con el consentimiento expreso del interesado o ser autorizado por el titular del órgano jurisdiccional, en resolución motivada"*.





de protección de datos en las sentencias de mayor calado cuando el acceso a su texto se realizara por terceros que cuando se realizara en el seno del proceso.

*3.2.2. "Anonimización" y "perjudicados": dos términos sin definición legal y un nuevo galimatías obligacional*

Si la conclusión que estamos esbozando en el estudio es que la obligación general es la seudonimización de datos personales tanto *ad intra* como *ad extra*[27], excepto cuando se trate de *"perjudicados"* a los que les alcanzaría una obligación mayor[28], la de anonimización de datos personales, el siguiente problema que se presenta es ¿quiénes son los perjudicados respecto de los que existiría la obligación de anonimización de datos?

Como viene siendo habitual en la materia que estamos tratando, las normas no aclaran la cuestión, ya que no se contiene ni en el RGPD, ni en la LOPD, ni en la LOPJ, ni en la LRJS, ni en la LEC, ninguna referencia que permita identificar quiénes podrían quedar encuadrados en dicho término. Recurriendo, nuevamente, al Diccionario de la RAE, *"perjudicado"* es quien "ha sido víctima de daño o menoscabo material o moral". Por su parte, el Diccionario del Español Jurídico[29], contiene tres lemas que refieren al término: *"culpa exclusiva del perjudicado"*[30], *"perjudicado por el delito"*[31] y *"tercero perjudicado en el seguro de responsabilidad civil"*[32], ninguno de los cuales guardaría relación alguna con aspectos jurídicos laborales y por extensión con sentencias del orden jurisdiccional social[33].

Puesto que la ausencia de definición de perjudicado no permite identificar a qué personas alcanzaría la obligación de anonimización contemplada en el art. 212.2 LEC, la respuesta sólo puede darse desde el análisis de los datos personales respecto de los que la normativa exige una especial protección. Dicho de otro modo, la labor de anonimización debe realizarse respecto de perjudicados, entendiendo por tales no cualquier persona que pueda verse afectada negativamente por una resolución –sentencia, resolución del INSS, de la TGSS, del SEPE, etc.– que le es desfavorable, sino como una persona respecto de la que dicha resolución vincula datos necesitados de especial protección[34].

[27] NIETO MANIBARDO, E. "Anonimización…", *op. cit.* pág. 149, señala que *"quizás deberíamos pensar en utilizar el sustantivo "seudonimización" como lo que en realidad es, una derivación de "seudónimo", que significa ocultar con un nombre falso el suyo verdadero, y no en el sentido de suprimir información o asignar códigos tal como hace el legislador en relación a la protección de datos de carácter personal"*.

[28] UTRILLA HERNÁN, R. "Acceso a los datos…", *op, cit.* pág. 571, parece alcanzar dicha conclusión cuando afirma que *"Es evidente que los ficheros automatizados conteniendo el texto de las sentencias, no requerirán el consentimiento del interesado, pero sí podrán ser objeto del ejercicio del derecho de acceso y rectificación"*.

[29] Igualmente de la Real Academia Española.

[30] Que se define, en el ámbito civil, como la *"situación que se produce cuando los daños causado por un tercero son imputables exclusivamente a una acción u omisión del perjudicado por el evento dañoso, lo que exonera de responsabilidad patrimonial a aquel"*.

[31] Que se define, en el ámbito procesal, como *"sujeto pasivo del delito o de sus consecuencias perjudiciales. Puede coincidir con el ofendido por el delito o no ser así cuando no sea la víctima del mismos sino quien se ve dañado por circunstancias que acompañan o derivan de su comisión"*.

[32] Que se define en el ámbito mercantil como *"persona física o jurídica que tiene un crédito indemnizatorio frente al asegurado responsable"*.

[33] Los términos se asemejan más a conceptos penales, respecto de los que la LOPDP establece obligaciones de protección de datos personales adicionales.

[34] Existe la posibilidad de considerar "perjudicados" a los afectados por procesos penales a los que refieren las obligaciones del art. 235 ter LOPJ, respecto de los que se instituyen reglas especiales respecto de la protección de datos. Puesto que el presente estudio se centra en las sentencias del orden jurisdiccional social, queda fuera del mismo el análisis de dicha cuestión. ORENES RUIZ, J.C. "Publicidad de sentencias, internet y protección de datos de carácter personal", *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 30, 2012, págs. 72, parece alcanzar idéntica conclusión cuando afirma que en realidad el termino debería entenderse en el sentido de *"condenado"*.





*3.2.3. La solución: la "seudonimización" como regla general y la "anonimización" de datos de categoría especial con efectos "ad extra"*

Si como se ha avanzado, la seudonimización de datos personales en las sentencias es la regla general con efectos *ad intra* y *ad extra*, para resolver la cuestión de qué datos deben ser objeto de anonimización, se debe recurrirse a una interpretación teleológica, sistemática e integradora de las normas que regulan la cuestión, ya que sólo así se podrá solventar el galimatías obligacional que rodea a la anonimización.

El RGPD prohíbe, en su art. 9, el tratamiento de determinados datos personales que considera de "categorías especiales". Así, prohíbe el tratamiento de datos que *"revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física"*. Y en parecidos términos se pronuncia la LOPD, que identifica a éstos con los datos *"cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico"*.

Por su parte, el tratamiento se define, en el art. 4.2) RGPD, como *"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"*[35].

Examinando conjuntamente la obligación –prohibición de tratamiento de datos de categoría especial– con la definición –tratamiento–, parecería que ni siquiera sería posible la recogida y registro de dichos datos, y por supuesto tampoco la conservación, consulta o comunicación de información relativa a datos que entraran en la categoría de datos especiales. Ello nos lleva a un nuevo absurdo en el ámbito de las obligaciones de protección de datos en las sentencias, ya que la información contenida en éstas –especialmente respecto de datos personales–, que puede ser utilizada *ad intra* o *ad extra*, puede ser identificada con un dato de los considerados de categoría especial, y dicho dato puede ser el eje sobre el que gire el proceso, lo que nos lleva a preguntarnos: ¿permite la anonimización con efectos *ad intra* resolver el proceso y garantizar el derecho a la tutela judicial efectiva de las partes? Pongamos un ejemplo, un trabajador puede presentar demanda porque considere que ha sido despedido por la pertenencia a un sindicato, pretendiendo en el proceso que se declare la nulidad del despido por vulneración del derecho fundamental a la libertad sindical precisamente por la afiliación a un sindicato en particular. La anonimización de dicho dato –pertenencia al sindicato X por ejemplo–, podría impedir la resolución de la controversia –por comparación, por ejemplo, con las sanciones distintas del despido impuestas a afiliados a los sindicatos Y o Z–, por lo que la anonimización del dato podría, incluso, vulnerar su derecho a la tutela judicial efectiva, al ser imposible resolver su pretensión. Un ejemplo más sencillo: el proceso puede girar sobre la calificación de un despido que tiene como causa la orientación sexual del trabajador ¿permitiría la anonimizacion de dicho dato resolver si el despido es nulo o no?

Intentemos resolver el galimatías. Al igual que anteriormente concluimos que no existía una obligación diferenciada respecto de la protección de datos de las sentencias *ad intra* y *ad extra*, ya que en cualquier caso lo que se impondría sería la seudonimización de los datos personales

[35] Sobre un estudio de la cuestión, si bien desde el prisma que estamos abordando pero en el marco de las sentencias dictadas por el Tribunal Constitucional, *vid.* GARCÍA HERRERA, V. "Transparencia jurisdiccional…", *op. cit.* pág. 5.

en cualquier caso, cuando se trate de un dato de carácter especial, la anonimización debería ser la regla general –eliminar el dato–pero sólo con efectos *ad extra*, es decir, respecto de terceros ajenos al proceso, pero nunca para las partes en el mismo y tampoco para los órganos jurisdiccionales que debieran conocer de las demandas o recursos.

Dicha conclusión tiene cobijo en la regulación legal de las obligaciones de tratamiento de datos en las sentencias. El propio art. 9.2 RGPD nos alumbra la solución. El apartado f) establece una excepción a la prohibición del tratamiento de dichos datos de carácter especial cuando *"el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial"*. El precepto, claramente, establece la excepción, pero en lo que en el ámbito de este trabajo estamos denominando tratamiento de datos personales *ad intra.* Es decir, cuando el art. 212.2 LEC refiere a la *"garantía del anonimato de los perjudicados"*, dicha garantía –anonimización– sólo surte efectos –en virtud de la excepción del art. 9.2 RGPD– *ad extra*, es decir, respecto del acceso a las sentencias por parte de terceros ajenos al proceso, anonimización que sólo afectaría a los que en el art. 9 RGPD se identifican como datos de categoría especial, mientras que respecto del resto de datos, la regla general se mantendría, ya que lo que habría que realizar es un proceso de seudonimización.

En conclusión: se deben seudonimizar, con carácter general, los datos personales de las personas físicas que contengan las sentencias, debiéndose anonimizar con efectos *ad extra* cuando se trate de datos personales de categoría especial identificados en el art. 9 RGPD.

4. DATOS PERSONALES SUSCEPTIBLES DE SEUDONIMIZACIÓN Y ANONIMIZACIÓN

Resueltos los dos galimatías:1) El que deriva de los distintos términos utilizados en las normas para lo que en apariencia es una misma obligación, que hemos resuelto en el sentido de que en realidad los cinco términos utilizados: seudonimización, minimización de datos, cifrado de datos –todos ellos utilizados en el RGPD–, anonimización –utilizado tanto en el RGPD como en la LEC–, disociación de datos y supresión de datos –utilizados por la LOPJ y la LEC– se encuadrarían en sólo dos categorías: A) seudonimización –que englobaría la minimización de datos, el cifrado de datos y la disociación de datos– y B) anonimización –que englobaría a la supresión de datos–, y 2) El galimatías obligacional provocado por la indeterminación de cuándo debe procederse a la seudonimización –respecto de datos personales que no se integren en la categoría de especiales–, y cuándo a la anonimización –respecto de datos personales de categoría especial, con efectos únicamente *ad extra*–, queda una nueva cuestión por resolver: ¿qué datos personales deben ser objeto de seudonimización en las sentencias?

Desde luego, y por exclusión, la seudonimización no alcanzaría a los datos personales que se identifiquen como de categoría especial –los que relacionaba el art. 9 RGPD–, puesto que respecto de ellos procedería la anonimización como antes se avanzó, y únicamente con efectos *ad extra* –respecto de terceros ajenos al procedimiento–, siendo necesaria la seudonimización respecto del resto de datos personales. Pero ¿cuáles son éstos?

Ni la normativa comunitaria ni la nacional concretan qué datos deben ser objeto de seudonimización, lo que en la práctica permite que los sujetos encargados de garantizar la protección de datos personales en las sentencias –Letrados de la Administración de Justicia[36], y órganos a los que el Consejo General del Poder Judicial atribuye dicha función– sean los que decidan qué datos pueden ser considerados sensibles y ser susceptibles de seudonimización o anonimización. Como posteriormente se examinará, no son pocos los problemas que derivan de una falta de concreción de qué datos deben considerarse personales, por lo que sirva un primer intento de sistematización que no obstante no supondrá un *númerus clausus.*

[36] Ya que los funcionarios de la oficina judicial tendrían asumidas funciones de seudonimización o anonimización pero no de los datos de las sentencias, sino de otras resoluciones dictadas en el seno del proceso (por ejemplo, actos de comunicación) que excede del ámbito del presente estudio.





El RGPD no hace más que oscurecer aún más la indagación de qué datos son personales cuando concreta que éstos son *"toda información sobre una persona física identificada o identificable"*, añadiendo que *"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"*. En un intento de reducción al mínimo de dicha definición, datos personales serían todos aquellos que permitieran identificar a una persona física, lo que puede hacerse sin esfuerzo alguno –directamente– o a través de una serie de datos de los que posteriormente se podría deducir a qué persona refieren –indirectamente–.

Parece claro que dato personal será el nombre y apellidos de la persona y las imágenes de dicha persona, pero también otros de los que se pueda identificar ésta, como DNI, número de pasaporte, número de la Seguridad Social, etc. Además, en el ámbito laboral existen datos que permitirían identificar a la persona aunque no fuera directamente. Pongamos un ejemplo, si una sentencia refiere al director general, los trabajadores de la empresa tendrían claro a qué persona refiere aunque se hubiera seudonimizado el nombre, y lo mismo ocurriría si por ejemplo la sentencia refiere al pescadero del supermercado, o a la secretaria del director, puesto que los compañeros de trabajo tendrían claro quiénes son las personas a que refieren. Si la obligación se extiende a dichos datos, deberían por lo tanto también seudonimizarse datos como la categoría profesional, la antigüedad, el salario, etc. En la práctica, y como posteriormente examinaremos, una seudonimización de dichos datos dificultaría –si no impediría– el ejercicio de funciones jurisdiccionales, por lo que se hace preciso reflexionar sobre cómo deba llevarse a cabo el tratamiento de dichos datos.

La única solución posible es la que hemos avanzado anteriormente. En ningún caso deberían ni seudonimizarse ni anonimizarse datos personales cuando los mismos aparezcan en sentencias y éstas no vayan a ser objeto de utilización por terceras partes en el proceso. Dicho de otro modo, la sentencia deberá notificarse a las partes con nombres, apellidos, y todos y cada uno de los datos personales que contenga, aunque pudieran ser objeto de seudonimización o anonimización. Igualmente, tampoco deberían ni anonimizarse ni sudonimizarse los datos cuando la sentencia se tenga que remitir a un órgano jurisdiccional diferente como consecuencia del planteamiento de un recurso contra dicha sentencia. La razón es simple, sin dichos datos, no sería posible el ejercicio de funciones jurisdiccionales encomendadas a jueces y tribunales.

Por el contrario, la seudonimización deberá realizarse, siempre, cuando las sentencias se hagan públicas y respecto de terceros ajenos al proceso, anonimizándose los datos que entren en la categoría de especiales, para que en ningún caso pudiera llegarse a conocer el mismo. Para terminar con un ejemplo. Si una sentencia declara la nulidad del despido por discriminación (por ejemplo porque la persona es homosexual), se seudonimizarían los datos personales (nombre, apellidos, categoría, etc.); como la seudonimización no impide totalmente el conocimiento de dichos datos, ya que como se expuso, a través de operaciones complejas podría llegarse a averiguar la persona a la que refiere, el dato relativo a su orientación sexual debería ser objeto de anonimización, ya que aunque llegara a conocerse a dicha persona, en ningún caso podría averiguarse que la discriminación ha sido por ser homosexual.

Dicha solución es perfectamente acorde con los mandatos del art. 9 f) RGPD, que admite como excepción del tratamiento de datos personales que hemos considerado de categoría especial, cuando *"el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial"*, lo que claramente refiere a la no seudonimización o anonimización de datos personales en lo que en este estudio hemos denominado con efectos *ad intra*.





5. PROBLEMAS PRÁCTICOS DE LA SEUDONIMIZACIÓN Y LA ANONIMIZACIÓN Y SUS SOLUCIONES

Como consecuencia de las dificultades que plantea una normativa confusa respecto de cómo se tiene que garantizar la protección de datos personales en las sentencias, bien por los problemas terminológicos que impiden saber con exactitud cómo se debe garantizar el derecho, bien por la imprecisión respecto de las obligaciones que incumben a los encargados del tratamiento de los datos de las sentencias, bien por la imprecisión de qué datos deben ser objeto de seudonimización o anonimización, bien por la falta de instrucciones claras acerca por los organismos competentes acerca de cómo se tiene que garantizar el derecho a la intimidad en las resoluciones judiciales, la realidad es que actualmente no son pocos los problemas reales que se derivan de un desconocimiento y/o mala utilización de mecanismos de seudonimización o anonimización. Si el presente estudio pretende arrojar una cierta luz sobre cuáles son dichas obligaciones, no puede cerrarse éste sin aventurar soluciones a los problemas reales a los que se ha enfrendado la autora del presente estudio en su trabajo diario como Letrada del Gabinete Técnico del Tribunal Supremo[37].

**5.1. Problemas derivados de la seudonimización y anonimización de datos personales contenidos en sentencias objeto de recurso**

Formando parte del derecho a la tutela judicial efectiva garantizado en el art. 24.1 CE, está el derecho al acceso a los recursos frente a sentencias. Dejando aparte los recursos de reposición y queja, que caben contra providencias, autos, diligencias de ordenación y decretos, y que por no suponer recursos contra sentencias escapan al ámbito del presente estudio, frente a las sentencias dictadas en instancia por los Juzgados de lo Social, así como contra los autos y sentencias que puedan dictar los Jueces de lo Mercantil que afecten al derecho laboral, cabe recurso de suplicación ante la Sala de lo Social del Tribunal Superior de Justicia[38]. Frente a las sentencias dictadas en única instancia por las Salas de lo Social de los Tribunales Superiores de Justicia, cabe recurso de casación ante la Sala 4ª del Tribunal Supremo[39]. Y frente a las sentencias dictadas por las Salas de lo Social de los Tribunales Superiores de Justicia en suplicación, cabe recurso de casación para la unificación de doctrina, igualmente ante la Sala 4ª del Tribunal Supremo[40].

Como consecuencia de las dificultades de conocimiento de las obligaciones de protección de datos personales contenidos en las sentencias, no son pocos los problemas que plantea el recurso a técnicas de sedudonimización o anonimización de datos personales en sentencias frente a las que se ha presentado un recurso. Es por ello que parece conveniente examinar qué se está haciendo en la práctica, qué problemas ocasiona una defectuosa aplicación de la normativa de protección de datos, y cómo pueden solventarse éstos para garantizar el derecho a la tutela judicial efectiva.

[37] Las funciones del Gabinete Técnico del Tribunal Supremo aparecen identificadas en el art. 61 bis 1 LOPJ, que *incluye la asistencia "a la Presidencia y a sus diferentes Salas en los procesos de admisión de los asuntos de que conozcan y mediante la elaboración de estudios e informes que se soliciten"*. Los Letrados del Gabinete Técnico son *"miembros de la Carrera judicial y otros juristas"* –art. 61 bis 2– que *"prestarán sus servicios en las diferentes áreas atendiendo a su especialización profesional"* –art. 61 bis 3 segundo párrafo–, siendo seleccionados "mediante concurso de méritos" –art. 61 quáter 2– de entre los *"funcionarios del Cuerpo de letrados de la Administración de Justicia o funcionarios de las Administraciones Públicas u órganos constitucionales, con titulación en Derecho, pertenecientes a Cuerpos del Subgrupo A1 o asimilados"* –art. 61 quáter 2 segundo párrafo.
[38] Regulado en el Libro Tercero, Título II, arts. 190 a 204 LRJS.
[39] Regulado en el Libro Tercero, Título III, arts. 205 a 217 LRJS.
[40] Regulado en el Libro Tercero, Título IV, arts. 218 a 228 LRJS.





*5.1.1. La no seudonimización o anonimización de datos personales de las sentencias recurridas*

Puesto que de recursos frente a sentencias se trata, el órgano jurisdiccional encargado de conocer del mismo debe conocer del texto íntegro de la sentencia para garantizar el derecho a la tutela judicial efectiva de las partes. Hasta el momento, en estos supuestos –y salvo raras excepciones–, se remiten las actuaciones por el órgano inferior al superior sin seudonimizar o anonimizar datos personales, por lo que, siguiendo con la línea abordada en el presente estudio, se estaría cumpliendo con la normativa de protección de datos que permite que con efectos *ad intra,* no se seudonimicen ni anonimicen datos personales contenidos en las sentencias, para garantizar el derecho a la tutela judicial efectiva de las partes y para cumplir con el mandato constitucional de ejercer *"la potestad jurisdiccional en todo tipo de procesos, juzgando y haciendo ejecutar lo juzgado"* –art. 117.1 LRJS.

En definitiva, como se avanzó en el presente estudio, la normativa deja margen para que no tengan que seudonimizarse ni anonimizarse datos de las sentencias cuando éstas sean objeto de recurso, ya que conforme al art. 9 f) RGPD, no está prohibido el tratamiento de datos cuando *"es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial"*, lo que se reitera en el art. 2 LOPDP[41]. Ello conlleva que no se tenga seudonimizar dato alguno, pero tampoco anonimizar aquellos datos que pertenezcan a la categoría de especiales, o que refieran a perjudicados, y ello por cuanto dichos datos sirven al ejercicio de funciones jurisdiccionales y por lo tanto tienen efectos *ad intra*.

*5.1.2. La seudonimización y anonimización de datos personales en sentencias invocadas de contraste en los recursos de casación para la unificación de doctrina*

El problema se presenta cuando, en determinados recursos, para hacer efectiva la garantía del derecho a la intimidad mediante la seudonimización o aninimización de datos personales, se exige que el órgano jurisdiccional conozca no sólo de la sentencia frente a la que se interpone recurso, sino también de otras sin las que el recurso no tendría sentido. Éste es el supuesto del recurso de casación para la unificación de doctrina (en adelante RCUD), en el que, conforme al art. 219 LRJS, se exige que exista contradicción entre sentencias respecto de *"los mismos litigantes u otros diferentes en idéntica situación donde, en mérito a hechos, fundamentos y pretensiones sustancialmente iguales se hubiere llegado a pronunciamientos distintos"*. Es decir, el RCUD sólo se admitirá cuando exista contradicción entre sentencias, lo que obliga a comparar hechos, fundamentos y pretensiones de las sentencias recurrida y de contraste. Los hechos probados de las sentencias que se someten a comparación con la recurrida, pueden contener datos de carácter personal, y en cuanto que tales, respecto de dichos datos deben proyectarse las obligaciones contempladas en la normativa reguladora de la protección de datos –RGPD, LOPDP, LOPJ, LEC–, entre ellas la suedonimización o anonimización de dichos datos.

Dada la indeterminación de si el conocimiento de dichas sentencias es con efectos *ad intra* o *ad extra*, provoca que se hayan aplicado técnicas de seudonimización y anonimización de datos personales en el texto de las sentencias que se remiten a la Sala 4ª del Tribunal Supremo a efectos de que éste, de apreciar identidad en hechos, fundamentos y pretensiones de las sentencias recurrida y de contraste, resuelva el RCUD presentado, lo que en la práctica provoca no pocos problemas.

[41] Cuando concreta que *"El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro d lea gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (…) y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 671985, de 1 de julio, del Poder Judicial, que le sean aplicables"*.

En la actualidad, los problemas derivan de dos circunstancias: 1) La consideración de que las sentencias que se remiten a la Sala 4ª del Tribunal Supremo en el marco del RCUD como sentencias invocadas de contraste por los recurrentes, se remiten con efectos *ad extra*, es decir, al margen del ejercicio de funciones jurisdiccionales, y como si la Sala 4ª fuera un tercero ajeno al proceso; y 2) La anonimización, *de facto*, de datos, que impide la tramitación del RCUD.

Respecto del primero, es preciso señalar que yerran los Letrados de la Administración de Justicia de los Tribunales Superiores de Justicia, cuando remiten certificaciones de sentencias que los recurrentes en casación para la unificación de doctrina han invocado de contraste en un RCUD, con datos seudonimizados o anonimizados. Puesto que no es posible el ejercicio de la función atribuida a la Sala 4.ª del TS de unificar doctrina cuando no es posible conocer datos sin los cuales sería imposible la realización de la averiguación de si los hechos probados de la sentencia recurrida y de contraste son sustancialmente iguales, la remisión de dichas sentencias no es con efectos *ad extra* –a un tercero ajeno al proceso– sino *ad intra* –en cuanto que se integraría en la dinámica del RCUD y por lo tanto el conocimiento de los datos personales de dichas sentencias serviría al ejercicio de la función jurisdiccional. Si, como se ha avanzado, la normativa permite que no se seudonimicen o anonimicen datos personales contenidos en sentencias cuando sea con efectos *ad intra*, no se entiende la razón por la que ello se está realizando en el marco del RCUD.

En conclusión, no se deberían seudonimizar o anonimizar datos personales de las sentencias que se remitan a la Sala 4.ª del Tribunal Supremo cuando se invoquen como sentencias de contraste en un RCUD.

Eliminado el primer obstáculo, no parecería necesario abordar el segundo, el derivado de la forma en que se está llevando a cabo la garantía del derecho a la intimidad de las personas físicas a las que refería el proceso, ya que la misma estaría excepcionada por la garantía del derecho a la tutela judicial efectiva de las partes, pero sirva su examen para demostrar cómo una interpretación de la normativa de protección de datos contraria a la alcanzada en el presente estudio, eliminaría el derecho a la tutela judicial efectiva de las partes en el proceso.

Los problemas derivados de dicha labor de seudonimizacion y anonimización, proceden: 1) de la falta de concreción de qué datos deberían ser objeto de seudonimización o anonimización, lo que permite el Letrado de la Administración de Justicia elegir los datos que considera personales y respecto de los que va a proceder a realizar alguna de esas dos labores, y 2) de la falta de instrucciones acerca de la forma en que debería llevarse a cabo dicha labor de seudonimización o anonimización. En la práctica, cuando se certifican sentencias invocadas de contraste en un RCUD, se está procediendo a eliminar datos necesarios para la resolución del mismo –se sustituye el dato por "(…)"– o a sustituir dichos datos por puntos suspensivos –*"(…)"*–, lo que *de facto* supone anonimizar dichos datos, ya que la Sala 4ª no podría, ni siquiera a través de operaciones complejas, llegar a conocer de dicho dato. Si además dicho dato es necesario para la resolución del RCUD, la vulneración del derecho a la tutela judicial efectiva está garantizada.

Abordemos los problemas con algunos ejemplos: 1) Como consecuencia de la falta de concreción de los datos que deberían ser objeto de seudonimización o anonimización, se han remitido a la Sala 4ª del Tribunal Supremo sentencias que sustituyen la fecha de nacimiento de un trabajador con "(…)", y ello en la consideración de que dicho dato es personal, y en cumplimiento de la normativa sobre protección de datos, el mismo debería ser seudonimizado o anonimizado. Ello ha provocado –por seguir con el ejemplo– que no sea posible conocer si el trabajador tenía la edad necesaria para acceder a la pensión de jubilación anticipada, dato determinante para la resolución de la controversia en suplicación, impidiendo comparar dicho dato con el de la sentencia frente a la que se plantea RCUD, y provocando que la Sala 4ª del Tribunal Supremo pueda realizar la labor de unificación otorgada ¿Es verdaderamente la fecha de nacimiento del trabajador un dato personal que deba ser objeto de seudonimiación o anonimización?; 2) Como consecuencia de la falta de indicaciones acerca de cómo debería realizarse la seudonimización o anonimización del dato, se han remitido a la Sala 4ª sentencias invocadas





de contraste en un RCUD, con la eliminación del nombre de empresarios personas físicas –dato que parece claro debería ser objeto de seudonimización o anonimización por ser el que más directamente vincula el dato con la persona–, lo que impide conocer a cuál de las personas a las que se corresponden los datos eliminados se está condenando efectivamente cuando se imponen determinadas responsabilidades. En la práctica, ello impide conocer cómo se articula la cadena de empresarios a los que se atribuye la efectiva prestación de servicios por parte del trabajador, y hace ininteligible la sentencia ¿Debería anonimizarse *de facto* el dato del nombre de la persona física del empresario, o bastaría con una simple seudonimización del mismo para no impedir la lectura ordenada de la sentencia y la concreción de las razones por las que el empresario persona física ha sido condenada? Al menos si el Letrado de la Administración de Justicia hubiera sustituido el dato por iniciales –seudonimizarlo–, en lugar de eliminarlo –anonimizarlo– sería posible que el Tribunal Supremo pudiera leer ordenadamente la sentencia permitiéndole comparar hechos probados de la sentencia recurrida y de contraste.

Dichos ejemplos son sólo la punta del iceberg de los problemas que está ocasionando la seudonimización o anonimización de datos en las sentencias remitidas a la Sala 4ª del Tribunal Supremo e invocadas como sentencias de contraste en los RCUD, problema que lleva al absurdo, por cuanto en realidad la sentencia invocada de contraste se remite, como avanzamos, con efectos *ad intra*, y el conocimiento de dichos datos es no sólo necesario, sino imprescindible para que la Sala 4.ª del Tribunal Supremo pueda llevar a cabo su función unificadora.

**5.2. Problemas derivados de la expedición de certificación literal de sentencias seudonimizadas o anonimizadas**

El art. 212.4 LEC concreta que *"los Letrados de la Administración de Justicia pondrán en los autos certificación literal de las sentencias y demás resoluciones definitivas"*. La certificación de sentencias se realiza a varios efectos: 1) *ad intra*, es decir, a efectos, por ejemplo, de remitirlas a la Sala 4ª del Tribunal Supremo por cuanto se han invocado de contraste en un RCUD; y 2) *ad extra*, cuando se solicita por terceros a los efectos que sea.

Es comprensible que los Letrados de la Administración de Justicia (en adelante LAJ), cuando reciben una solicitud de sentencia, aunque sea a los efectos de un RCUD, entiendan que la sentencia se solicita por un tercero ajeno al proceso –*ad extra*–, y por lo tanto piensen que están obligados a cumplir con los mandatos del RGPD, LOPDP, LOPJ y LEC, procediendo a la anonimización o seudonimización de los datos peronales contenidos en las sentencias, sin embargo, como ya hemos avanzado, no sería necesaria dicha labor, al menos siempre, ya que sólo procedería la seudonimización o anonimización pero con efectos *ad extra*, es decir respecto de partes ajenas al proceso y cuando dichas partes no necesiten dichas sentencias a efectos jurisdiccionales, lo que ocurre cuando se solicita la certificación de la misma a efectos del recurso de casación para la unificación de doctrina.

En cualquier caso, la práctica demuestra que cuando se expide una certificación de sentencia por los LAJ, la misma se expide seudonimizada o anonimizada, si bien especifican que la misma es *"certificación literal"*, incluyendo en el texto que la certificación *"concuerda fielmente con el original"*, aun cuando ello no es cierto por cuanto la sentencia está seudonimizada o anonimizada.

Para evitar el problema de certificar algo que no es cierto, el texto de la certificación debería ser de un tenor diferente. Algunos LAJ ya están incorporando a las certificaciones textos que evitarían el problema anteriormente presentado, por lo que se propone el siguiente modelo: la presente sentencia concuerda fielmente con el original, excepto en relación con los datos de carácter personal que por mandato de la normativa de protección de datos deben estar seudonimizados, y ello en cumplimiento de la obligación de que la difusión del texto de esta resolución a partes no interesadas en el proceso en el que ha sido dictada, sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, con ad-





vertencia de que respecto de las partes en el proceso, los datos personales incluidos en esta resolución no podrán ser cedidos ni comunicados con fines contrarios a las leyes.

Una segunda solución al problema sería certificar no las sentencias que aparecen en el libro de sentencias, y que como no puede ser de otro modo no están seudonomizadas o anonimizadas, sino las sentencias que aparecen ya seudonimizadas o anonimizadas por el CENDOJ. Ello sin embargo acarrea dos problemas adicionales: 1) El primero tiene que ver con el tiempo que tarda el CENDOJ en seudonimizar o anonimizar las sentencias, de forma que como dicha labor no se realiza de forma automática, la dilación en llevar a cabo dicho proceso podría perjudicar a la parte que necesita, para no incumplir los plazos procesales para interponer recurso, por ejemplo, dicha sentencia seudonimizada o anonimizada rápidamente; 2) El segundo tiene que ver con que la certificación ya no sería *"literal"* de las sentencias que se dicten por el órgano jurisdiccional respecto del que el LAJ tiene la obligación de certificación de dicha sentencia, sino que sería una certificación de una sentencia publicada en el CENDOJ, lo que los LAJ podrían considerar queda extramuros de la obligación impuesta por el art. 212.4 LEC. Ello no es así, lo que el precepto contempla es la obligación de poner *"en los autos certificación literal de las sentencias y demás resoluciones definitivas"*, sin que el mismo concrete que deban ser las que aparecen en el libro de sentencias, por lo que esta segunda solución, también, podría ser eficaz a los efectos que estamos examinando. Si se optara por esta segunda fórmula, debería incorporarse como texto de la certificación: en cumplimiento de la normativa de protección de datos, y puesto que la presente certificación se expide a solicitud de una parte ajena al proceso, se procede a certificar la sentencia conforme a la seudonimización y anonimización de datos personales realizada por el Consejo General del Poder Judicial a través del CENDOJ.

**5.3. Problemas derivados de la seudonimización o anonimización de los nombres de los abogados**

Un tercer problema que plantea el cumplimiento de la obligación de datos personales en las sentencias, cuando dicha labor se realiza incluso con efectos *ad intra* –que como estamos defendiendo no procedería–, es que puesto que los abogados que representan a las partes son personas físicas, se están seudonimizando o anonimizando los nombres y apellidos de los abogados intervinientes en el proceso. Ello ha ocasionado cierta preocupación por las consecuencias que dicha seudonimización o anonimización provoca: 1) El primero es que si se expidiera una certificación de la sentencia con sus datos anonimizados o seudonimizados, no sería posible que éstos justificaran ante sus clientes su intervención en el proceso, o a futuros clientes su buena labor en el ejercicio de sus funciones de representación legal, lo que le impediría mantener a antiguos clientes u obtener nuevos; 2) El segundo es que la labor de representación legal en juicio tiene consecuencias respecto de la trayectoria profesional de los abogados, por ejemplo, a efectos de poder acceder al cuarto turno en cuanto que letrados de reconocido prestigio, ya que la anonimización de sus datos impediría conocer del número de procedimientos en los que han participado o del éxito de su labor en los mismos, impidiéndoles, *de facto*, poder acreditar méritos suficientes.

La solución al problema sólo puede encontrarse de dos formas: 1) Pidiendo anticipadamente a los abogados autorización para que sus nombres consten en las sentencias en las que han asistido como representantes legales de sus clientes –ya que en determinados procedimientos su nombre podría aparecer pero como parte del proceso, en cuyo caso sería necesaria la seudonimización o anonimización de su nombre o datos personales con efectos *ad extra*–, o 2) No se debería seudonimizar o anonimizar dicho dato en la sentencia, salvo que ellos mismos notificaran, en el ejercicio de los derechos ARCO, que debería procederse a dicha seudonomización o anonimización.

**5.4. Las soluciones**

Al hilo de los problemas que hemos ido esbozando –y que son sólo ejemplos, porque existirían otros muchos que por motivos de extensión no han podido ser abordados en el presente





estudio– se han ido abordando también las soluciones, que pueden resumirse en dos: 1) No se deberían seudonimizar o anonimizar datos personales de sentencias con efectos *ad intra*, es decir, en el marco de la función jurisdiccional y entre partes del proceso o partes ajenas al proceso que requieren conocer de datos personales para garantizar su derecho a los recursos –por ejemplo de casación para la unificación de doctrina–; y 2) Se deberían dar instrucciones, bien mediante la aprobación de una norma específica respecto de la forma de llevar a cabo la seudonimización o anonimización de sentencias, bien por el CGPJ sobre los datos que deben ser objeto de seudonimización y anonimización y la forma en que debe realizarse ésta.

Siendo ello cierto, dichas soluciones son de fácil implantación en la práctica, y ello por cuanto el propio CGPJ tiene instrucciones concretas sobre cómo se tiene que llevar a cabo la seudonimización o anonimizacion de sentencias a efectos de su difusión por el CENDOJ. Éste es el órgano encargado de la seudonimización o anonimización de datos personales en las sentencias que se publican en su base de datos, y la forma en que lleva a cabo dicha labor debería hacerse extensible a todos los órganos jurisdiccionales y respecto de todas las personas encargadas del tratamiento de datos, incluidos los LAJ que deban certificar sentencias.

A efectos ilustrativos, señalar que la labor de seudonimización o anonimización se realiza modificando los nombres de las personas físicas que aparecen en las sentencias, y eliminando datos –que sustituye con las letras *"NUM"*– a las que se añaden números en el formato 000 –*"001","002","003"*, etc.– de los que puede deducirse a qué persona refiere (por ejemplo, los códigos de puesto de trabajo, vuelos asignados a una azafata, números de pólizas, números de cotización, domicilio, número de la libreta de ahorro, etc.) eso sí, manteniendo el mismo nombre asignado cuando la sentencia refiere a dicha persona a lo largo de todo el texto y el mismo código cuando se refiere al mismo dato. Ello cumple con las exigencias de la normativa de protección de datos, y no impide una lectura ordenada de la sentencia y el conocimiento de los datos esenciales de la misma, por lo que el mismo esquema debería seguirse para seudonimizar o anonimizar datos personales por los responsables del tratamiento de datos de los órganos jurisdiccionales.

Siendo ello deseable, sería conveniente que el CGPJ estableciera procedimientos en que se concretaran: 1) Qué datos de las sentencias se consideran personales y por lo tanto tienen que ser objeto de seudonimización o anonimización –por ejemplo, si se tiene que seudonimizar la fecha de nacimiento de un trabajador, el nombre del abogado, etc.–; 2) Cómo debe llevarse a cabo la seudonimización o anonimización, para lo que serviría la remisión a los LAJ de las mismas instrucciones que se han dado al CENDOJ sobre cómo llevar a cabo la seudonimización y anonimización de sentencias; y 3) Dar publicidad y formación sobre las cuestiones anteriores a los sujetos encargados del tratamiento de datos personales de las sentencias –jueces, LAJ, funcionarios de la oficina judicial, etc.– para lo que podrían utilizarse los recursos de formación del CGPJ[42] para impartir cursos sobre *"Obligaciones de seudonimización o anonimización de datos en las sentencias del orden jurisdiccional social"*, y por extensión, y aunque no se ha abordado en el presente estudio sobre *"Obligaciones de seudonimización o anonimiziación de datos personales en el orden jurisdiccional social"*, lo que incluiría, también, las obligaciones que la normativa de protección de datos impone respecto de cualquier actuación llevada a cabo por el órgano jurisdiccional u oficina judicial –providencias, edictos, autos, etc.

[42] De hecho el presente estudio trae causa del *"Curso sobre protección de datos y relaciones laborales"*, organizado por el Consejo General del Poder Judicial en colaboración con la Asociación Española de Derecho del Trabajo y de la Seguridad Social, celebrado entre los días 22 a 24 de enero de 2020, y dirigidos por la Excma. Sra. Dª María Luisa Segoviano Astaburuaga, Magistrada de la Sala de lo Social del Tribunal Supremo y D. Guillermo L. Barrios Baudor, Catedrático de Derecho del Trabajo y de la Seguridad Social de la Universidad Rey Juan Carlos.

## 6. CONCLUSIONES

El Derecho originario de la UE sólo vincula la protección de datos personales a derechos fundamentales, principalmente el derecho a la intimidad, pero sin regular cómo debe garantizarse dicho derecho en el marco del proceso y especialmente respecto de datos personales contenidos en el texto de las sentencias. Por su parte, el RGPDP aclara que la protección alcanza solamente a las personas físicas y en el marco de *"actividades de los tribunales y otras autoridades judiciales"*, de lo que se deduce que se debe garantizar el derecho a la intimidad de las personas físicas a través de mecanismos que impidan vincular un dato a una persona en particular. Cómo deba llevarse a cabo dicha protección se convierte en un galimatías terminológico, al aludir el RGPDP a los términos: seudonimización, cifrado de datos, y anonimización –en este supuesto para excluir del RGPDP a la información anónima–, sin definir éstos y sin vincular obligaciones concretas a cada término.

El art. 18.4 CE obliga a limitar el uso de la informática para garantizar, entre otros, el derecho al honor y la intimidad, sin que la LOPDP, aprobada en desarrollo de dicho precepto, tampoco contemple regulación alguna acerca de cómo se deben garantizar los derechos en el marco del proceso y respecto de los datos personales contenidos en las sentencias. La primera referencia en el ordenamiento jurídico español se contiene en la LOPJ, cuyo art. 236 bis obliga a jueces y tribunales a cumplir con las obligaciones de tratamiento contempladas en el RGPD y LOPDP. La forma de articular la protección no es terminológicamente coincidente con la utilizada en el RGPD, al referir a la disociación de datos de carácter personal contenidos en las sentencias –art. 235 bis LOPJ– y a la supresión de datos personales de los documentos a los puedan acceder las partes durante la tramitación del proceso –art. 236 quinquies LOPJ.

En perspectiva iuslaboralista, la LRJS no contiene referencia alguna a la protección de datos en las sentencias, aunque sí aparece la misma en el art. 212.2. LEC, que alude a la disociación de datos de carácter personal y a la garantía del anonimato de los perjudicados, aclarándose, en el Reglamento 1/2005, del Consejo General del Poder Judicial, que el acceso a las sentencias no podrá afectar al derecho a la intimidad de las personas, estableciendo una especie de prohibición de acceso a datos de personas necesitadas de especial tutela y garantizando el anonimato de víctimas o perjudicados, sin definir quiénes son unas y otras.

Puede afirmarse con rotundidad, que el principal problema que plantea la protección de datos en sentencias es fundamentalmente terminológico, y provocado por la utilización de términos diferenciados, muchos de ellos no definidos, y no vinculados a obligaciones concretas que diferencien a unos de otros, lo que provoca un galimatías terminológico necesitado de aclaración. El presente estudio ha ofrecido definiciones de términos no definidos normativamente, pero sí enunciados en las normas reguladoras de la protección de datos, y no coincidentes; en particular: seudonimización, minimización de datos, cifrado de datos personales –enunciados en el RGPDP– anonimización –enunciada en el RGPDP y LOPJ–, y disociación de datos y supresión de datos –LOPJ y LEC.

Del examen de las definiciones se concluye que todos ellos pivotan sobre dos: 1) la seudonimización de datos personales, que se conseguiría mediante la minimización, el cifrado de datos –en términos del RGPD– o la disociación de datos –en términos de la LOPJ–, y 2) la anonimizacion de datos personales –en términos del RGPD y LEC–, que se conseguiría mediante la supresión de datos personales –en términos de la LEC.

Dicha reducción de cinco términos a dos, provoca no pocos problemas cuando se tienen que examinar las obligaciones que traerían aparejadas, por lo que una vez resuelto el galimatías terminológico, aparece un nuevo galimatías obligacional. El primero aparece cuando de una interpretación normativa podría deducirse que se estaría estableciendo una obligación de mayor calado –anonimización– cuando la sentencia se remite a las partes del proceso –lo que en este estudio se ha denominado con efectos *ad intra*–, que cuando el contenido de la sentencia se conoce por un tercero al proceso –lo que en este estudio se ha denominado con efectos *ad extra*–, respecto de que la que se establecería una obligación menor –seudonimización–.





La solución a dicho galimatías obligacional se aborda desde un análisis integrador, teleológico y sistemático de las normas, concluyéndose que la seudonimización de datos personales en las sentencias es la regla general y ello con efectos *ad intra* y *ad extra*, mientras que sólo se anonimizarían datos personales de quienes puedan considerarse *"perjudicados"* –en términos del art. 212.2 LEC– término no definido en norma alguna, y que en realidad se vincularía a datos de personas que se encuadren en lo que se identifica, esta vez sí, de forma expresa en el RGPD y en la LOPDP, con categorías especiales de datos –los que permitan identificar la persona con su ideología, afiliación sindical, religión, orientación sexual o vida sexual, creencias, origen racial o étnico, datos genéticos, biométricos o de salud. Ahora bien, dicha anonimización sólo procedería con efectos *ad extra*.

El segundo problema lo plantea la existencia de la propia obligación de anonimización de datos que puedan considerarse de categoría especial, ya que en el ámbito jurídico-laboral dichos datos pueden suponer la base misma del conflicto –un despido por la orientación sexual del trabajador, por ejemplo. La solución alcanzada en el presente estudio parte, nuevamente, de una interpretación conjunta de los arts. 9.2 RGPD y 212.2 LEC, que permite concluir que la anonimización sólo puede producirse con efectos *ad extra*, es decir, respecto de terceros ajenos al proceso, pero nunca para las partes en el mismo ni tampoco para los órganos jurisdiccionales que debieran conocer de las demandas o los recursos.

El tercer problema proviene de la falta de concreción de qué datos deben ser objeto de seudonimización en las sentencias y cómo tiene que llevarse a cabo la misma. Puesto que la normativa sobre protección de datos no aclara la cuestión, el presente estudio ha ofrecido un criterio de identificación de los mismos que sin embargo no supone un *númerus clausus*, y ha examinado la forma en que debe llevarse a cabo, concluyéndose, mediante el planteamiento de los problemas prácticos que se han sistematizado en el presente estudio, que: 1) Se debería aprobar una norma específica sobre cómo debe garantizarse la protección de datos personales contenidos en las sentencias; y 2) Se debería formar e informar a los sujetos responsables del tratamiento de datos sobre qué datos deben ser objeto de seudonimización –*ad intra* y *ad extra*–, y qué datos deben ser objeto de anonimización –*ad extra*–, y sobre la forma de realizar dicha seudonimización y anonimización.

El estudio aventura, además, cómo debe llevarse a cabo la seudonimización y la anonimización de datos personales, cómo deben realizarse las certificaciones de sentencias por los LAJ, qué cambios normativos debe incorporar el legislador y qué función debe asumir el CGPJ.

Planteados los problemas, sistematizadas las soluciones, sólo queda que las propuestas avanzadas en el presente estudio se acojan por quienes tienen competencia para regular la forma en que debe garantizarse el derecho a la intimidad de las partes en un proceso laboral, especialmente como consecuencia de la aparición de datos personales en las sentencias. Seamos optimistas.