
This is the **published version** of the bachelor thesis:

Álvaro Cazorla, Joel. *La cadena perpetua digital : El derecho al olvido como última garantía de la reinserción social y la dignidad humana*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Dret). 54 pàg.

This version is available at <https://ddd.uab.cat/record/331985>

under the terms of the  license.



Trabajo Fin de Grado

**LA CADENA PERPETUA DIGITAL:
El Derecho al Olvido como Última Garantía de la Reinserción
Social y la Dignidad Humana.**

Autor

Joel Alvaro Cazorla

Tutora:

Maria Del Carmen Gete-Alonso Calera

Grado en Derecho

FACULTAD DE DERECHO

Año 2025/2026

A Mami y Tata,

Si hoy estoy aquí, es por vosotros. Aunque el camino no siempre ha sido fácil y hayamos tenido momentos complicados, nunca nos hemos soltado de la mano. Hemos aprendido a levantarnos juntos, a reconstruirnos y a querernos incluso en los días más difíciles. Gracias por creer en mí cuando ni yo mismo sabía cómo hacerlo, por enseñarme que la vida no regala nada, pero que con amor todo pesa menos. Sois mi hogar, mi refugio y mi mayor motivo. Todo lo que soy, todo lo que he conseguido y todo lo que algún día llegaré a ser, nace de vosotros.

Este logro no es solo mío, es nuestro.

A Papi,

Aunque la vida nos haya llevado por caminos en los que no siempre hemos podido compartir todo lo que nos habría gustado, has estado presente de una forma que va más allá de la distancia. Has sido apoyo, guía y fuerza, incluso en silencio. Te quiero y, quiero que sepas que una parte de este trabajo, de este esfuerzo y de este sueño cumplido, también te pertenece.

A mis Yayos,

Sois la raíz de todo. Mi ejemplo, mi historia y mi mayor orgullo. Gracias por enseñarme con hechos lo que significa el esfuerzo, la humildad y el amor incondicional. Hoy puedo decir que he cumplido aquello que tanto soñabais: ser el abogado de la familia y, no sabéis lo que significa para mí poder escribiros esto. Yaya, sé que este momento lo habrías vivido como nadie. Me duele no poder abrazarte hoy, pero cuando miro al cielo siento que sigues aquí, acompañándome en cada paso. Tú me enseñaste lo que es el amor de verdad, y ojalá pudieras ver en lo que me he convertido. Todo lo que hago, lo hago también por ti. Sé que estarías orgullosa, y solo pensar en tu sonrisa es lo que me da fuerzas para seguir. Yayo, aquí me tienes, aunque a veces la memoria se escape, yo nunca voy a dejar que olvides cuánto te quiero. Eres parte de mí, de lo que soy, y lo serás siempre.

Y, por último, a mí,

Porque sé lo que ha costado llegar hasta aquí. Porque nadie conoce las noches difíciles, las dudas, el cansancio y las ganas de dejarlo todo que hubo en el camino. Por no rendirme cuando más fácil era hacerlo, por seguir adelante cuando todo pesaba demasiado y por levantarme una y otra vez. Hoy no solo termino un trabajo, hoy cierro una etapa de lucha, de esfuerzo y de superación.

Y hoy, por fin, puedo decir: lo he conseguido.

Abstract The digital era has transformed the paradigm of collective memory, turning remembrance into the norm and forgetting into the exception. This Bachelor's Thesis addresses the issue of the "digital life sentence" suffered by rehabilitated individuals, whose digital footprint continues to publicly link them to a past of addictions or criminal records that have already been overcome. The research analyzes the conflict between the right to information and the right to honor, focusing on how the passage of time alters the public relevance of news. Through a dogmatic methodology and the analysis of key jurisprudence, such as STJUE of May 13, 2014, the effectiveness of the Right to be Forgotten (Art. 17 GDPR) is examined as an instrumental tool to guarantee social reintegration (Art. 25.2 SC). The main hypothesis sustains that the indefinite validity of sensitive data on the internet violates human dignity and prevents effective rehabilitation, necessitating a more rigorous application of the data accuracy principle to protect the right to a second chance.

Palabras Clave: Derecho al olvido, cadena perpetua digital, reinserción social, desindexación, estigmatización algorítmica, protección de datos.

Resumen La era digital ha transformado el paradigma de la memoria colectiva, convirtiendo el recuerdo en la norma y el olvido en la excepción. Este Trabajo de Fin de Grado aborda la problemática de la "cadena perpetua digital" que sufren las personas rehabilitadas, cuya huella digital sigue vinculándolas públicamente a un pasado de adicciones o antecedentes penales ya superados. La investigación analiza la colisión entre el derecho a la información y el derecho al honor, centrándose en cómo el paso del tiempo altera la relevancia pública de la noticia. A través de una metodología dogmática y del análisis de jurisprudencia clave, como la STJUE de 13 de mayo de 2014, se examina la eficacia del Derecho al Olvido (Art. 17 RGPD) como herramienta instrumental para garantizar la reinserción social (Art. 25.2 CE). La hipótesis principal sostiene que la vigencia indefinida de datos sensibles en internet vulnera la dignidad humana e impide una rehabilitación efectiva, haciendo necesaria una aplicación más rigurosa del principio de calidad del dato para proteger el derecho a una segunda oportunidad.

Keywords: Right to be forgotten, digital life sentence, social reintegration, de-indexing, algorithmic stigma, data protection.

TABLA DE CONTENIDO

1. Introducción.....	6
1.1. Contextualización: El derecho al olvido como facultad de desindexación...	7
1.2. Justificación y relevancia social: La estigmatización algorítmica como barrera a la rehabilitación.....	10
1.3. Objetivos y metodología de la investigación.....	12
2. El Marco Constitucional: La Ponderación de Derechos Fundamentales....	14
2.1. Antecedentes normativos y jurisprudenciales del Derecho al Olvido.....	14
2.2. El derecho a la información (Art. 20.1.d CE): Requisitos de veracidad y la pérdida de "relevancia pública" por el paso del tiempo.....	17
2.3. El derecho al honor, la intimidad y el libre desarrollo de la personalidad (Arts. 18 y 10.1 CE) en el entorno digital.....	20
2.4. El concepto de "Hemeroteca Digital": Distinción jurídica entre la fuente original y la indexación en motores de búsqueda.....	25
3. La Reinserción Social frente a la Huella Digital.....	29
3.1. El mandato constitucional de reinserción (Art. 25.2 CE): Su aplicación extensiva más allá del ámbito penitenciario.....	30
3.2. La protección reforzada de datos sensibles: El tratamiento de datos de salud y adicciones (Art. 9 RGPD).....	31
3.3. La paradoja jurídica: La cancelación administrativa de antecedentes penales frente a la vigencia perpetua de la información en internet en el ámbito de acceso laboral.....	35
4. El Origen de la Doctrina: La STJUE de 13 de mayo de 2014.....	40
4.1. Análisis Jurisprudencial: Evolución y Criterios de Supresión.....	41
5. Conclusiones.....	45
6. Bibliografía y Referencias.	

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
ARCO	Derechos de Acceso, Rectificación, Cancelación y Oposición
CAP	Certificado de Antecedentes Penales
CE	Constitución Española de 1978
CEDH	Convenio Europeo de Derechos Humanos
CP	Código Penal
LOPD	Ley Orgánica 15/1999 de Protección de Datos Personales
LOPDGDD	Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales
LORTAD	Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
RGPD	Reglamento (UE) 2016/679 General de Protección de Datos
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea.

1. Introducción

El gran avance tecnológico que hemos experimentado durante las últimas décadas, especialmente con la revolución digital, ha provocado un cambio radical en nuestras costumbres. Internet no solo ha modificado nuestra forma de interactuar y comunicarnos, sino que ha alterado aspectos básicos de nuestra vida cotidiana: desde la manera en que consumimos información o trabajamos, hasta cómo construimos nuestra identidad personal y nuestras relaciones sociales.

Tradicionalmente, la limitación de los soportes físicos dificultaba el acceso a la información más antigua, lo que favorecía un olvido progresivo de los hechos que iban perdiendo relevancia. A raíz de esta evolución, se genera de forma automática una especie de “currículum personal” digital, provocando que este rastro no se limite a información actual o relevante, sino que arrastre datos antiguos accesibles prácticamente desde cualquier lugar del mundo o dispositivo digital, que deberían haber quedado en el olvido.

Esta imperfección de la memoria era, en realidad, una garantía para el ser humano, ya que le permitía evolucionar y redefinir su identidad sin el lastre permanente de sus errores o actos pasados que ya no representaba su ser actual.

En palabras de Ángela Moreno Bobadilla¹ “Antes de la creación de Internet, la memoria humana imperaba sobre la memoria virtual, provocando que el mero transcurso del tiempo convirtiera ciertos datos en irrelevantes”.

Sin embargo, la llegada de la Sociedad de la Información y, más recientemente, de la Sociedad del Dato, ha provocado una mutación de esta condición. Como han señalado grandes juristas como Stefano Rodotà², hemos pasado de una sociedad donde el control era físico y limitado, a una era de “vigilancia algorítmica”. Lo que provoca que la norma se invierta por completo: ahora lo natural es el recuerdo total y lo excepcional es el olvido.

¹ Moreno Bobadilla, Á. (2020). "El olvido previo a Internet: los orígenes del actual derecho al olvido digital". *Cuestiones Constitucionales*, n.º 43, p. 200.

² Rodotà, S. (2014). *El derecho a tener derechos* (J. M. Revuelta, Trad.). Editorial Trotta

Esta nueva realidad es la que genera la Cadena Perpetua Digital, especialmente grave para personas que han superado adicciones o han cumplido penas penales, ya que Internet les impide desprenderse de un pasado que la ley y la sociedad, técnicamente, ya les ha perdonado.

Por eso, este trabajo se centra específicamente en analizar la afectación que provoca esta memoria perpetua sobre dos casos muy delicados: los antecedentes penales ya cancelados y los datos médicos sobre adicciones. El objetivo principal es ver si las leyes actuales, como el RGPD o el mandato de reinserción de la Constitución, garantizan una protección real frente a la indexación perpetua de motores de búsqueda. La investigación busca demostrar que la dignidad humana exige que la identidad digital de una persona sea dinámica y veraz, evitando que un pasado ya superado se convierta en una barrera infranqueable para su desarrollo personal y profesional en el presente.

1.1. Contextualización: El derecho al olvido como facultad de desindexación.

Para comprender el alcance de esta investigación, es preciso definir qué entendemos por derecho al olvido, no delimitándolo a una pretensión de reescribir el pasado, sino como una herramienta jurídica para evitar que nuestra información personal siga circulando por internet si no cumple con los estándares normativos actuales. Lo que busca este derecho es dar la posibilidad a los individuos de limitar este rastro digital indiscriminado que generan los motores de búsqueda, especialmente cuando los datos han quedado obsoletos o carecen de relevancia pública. Lo más interesante jurídicamente es que esta protección no solo actúa contra publicaciones ilegales desde el inicio, sino también contra aquellas que, siendo lícitas en su origen, han perdido su razón de ser debido al paso del tiempo.

La Agencia Española de Protección de Datos³ (AEPD) lo define como "el derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa". En concreto, esta facultad permite limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información ha quedado obsoleta o carece de relevancia e interés público.

³ Agencia Española de Protección de Datos (AEPD). "Derecho al olvido"

En sintonía con esta visión, la doctrina especializada profundiza en la vertiente del control individual y la protección de la esfera privada. A este respecto, Inmaculada Jiménez Castellanos Ballesteros⁴, lo define como “la facultad que tiene una persona, de controlar y limitar la difusión actual de hechos verídicos de su pasado, acompañados de sus datos identificativos, que carecen de interés público vigente y afectan a su vida privada”. La citada autora precisa la dimensión práctica de esta pretensión jurídica de la siguiente manera: “El derecho al olvido digital se reivindica en relación con un determinado contenido obsoleto, referido a una persona privada, que ha sido divulgado en Internet y al que se accede a través de una búsqueda por el nombre y los apellidos. El afectado pretende, mediante el ejercicio de este derecho, impedir la difusión o indexación de aquella información que le perjudica o simplemente desea que sea olvidada.”

Esta idea fue reiterada y consagrada a nivel jurisprudencial por el Tribunal de Justicia de la Unión Europea en su resolución STJUE de 13 de mayo de 2014. Asunto C-131/12⁵ (Google Spain SL, Google Inc. contra Agencia Española de Protección de Datos y Mario Costeja González). Esta resolución, fue la encargada de reconocer el derecho del interesado a exigir a un motor de búsqueda que elimine de sus resultados los enlaces que derivaban a informaciones que, con el tiempo, le resultaban perjudiciales (Guichot, E, 2019)⁶.

A nivel normativo, este derecho encuentra su fundamento principal en el Artículo 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, conocido como “derecho de supresión”. Esta disposición europea se complementa en el ordenamiento jurídico español a través del Artículo 93 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que integra el derecho al olvido dentro del catálogo de los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

⁴ Jiménez-Castellanos Ballesteros, I. (2019). "El conflicto entre el derecho al olvido digital del pasado penal y las libertades informativas: las hemerotecas digitales". *Revista de Derecho Político*, n.º 106, p. 141-142.

⁵ Tribunal de Justicia de la Unión Europea. (2014, 13 de mayo). *Sentencia Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (Asunto C-131/12).

⁶ Guichot, E. (2019). El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español. *Revista de Administración Pública*, 209, 45-92.

Es crucial no confundir los distintos mecanismos jurídicos (Agencia Española de Protección de Datos AEPD, 2020)⁷ que prevé el artículo 17 del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD).

Por un lado, la supresión se entiende como la medida más drástica consistente en la eliminación física y definitiva de los datos de la fuente original, provocando que la información desaparezca por completo del servidor o base de datos donde fue publicada inicialmente.

La desindexación es la manifestación más común del derecho al olvido frente a los motores de búsqueda, esta facultad no elimina la información de la fuente original, sino que rompe el vínculo entre el nombre de una persona y en enlace de dicha información. En palabras de Ana Belén Casares Marcos “su ejercicio no suprime información en internet, sino tan solo bloquea los enlaces que los motores de búsqueda pudieran arrojar al rastrear a partir del nombre del interesado, siempre que no subsista interés público en que se mantengan accesibles a los internautas”.

Por último, en cuanto a la Anonimización, a diferencia de las anteriores técnicas, no se extiende como una herramienta jurídica para eliminar u ocultar la información, sino que pretende transformarla despojándola de tal manera que no pueda atribuirse a una persona identificada o identificable, pero preservando su utilidad para fines como por ejemplo históricos o estadísticos.

La distinción entre supresión, desindexación y Anonimización no es una mera cuestión conceptual, sino que constituye la clave fundamental para poder aplicar correctamente el derecho al olvido. Esta diferenciación es la que permite articular una solución jurídica equilibrada, capaz de ponderar los derechos que devienen en conflicto: por un lado, la protección de la dignidad y el libre desarrollo de la personalidad del individuo y, por otro, la libertad de información y la integridad de los archivos digitales, como las hemerotecas.

⁷ Agencia Española de Protección de Datos. (2020). *Informe 0057/2020 sobre el contenido del derecho al olvido previsto en el artículo 17 del Reglamento 2016/679 y el artículo 93 de la Ley Orgánica 3/2018*. Gabinete Jurídico de la AEPD.

Con la desindexación, se ataca directamente el foco problemático de la cadena perpetua digital, pero sin la necesidad de alterar o censurar la fuente original. De este modo, se protege al individuo del estigma perpetuo sin necesidad de reescribir la historia. En este sentido, resulta especialmente esclarecedora la aportación de Norberto Nuno Gomes de Andrade⁸, quien lo define como un pilar para la reconstrucción personal al establecer que

“El derecho a ser olvidado también equivale al derecho a un nuevo comienzo, el derecho a empezar de nuevo desde cero y el derecho a la autodefinición, que evita que el pasado condicione (de una manera excesiva) nuestra vida presente y futura. El derecho a ser olvidado, por tanto, se considera un instrumento jurídico importante para deconstruir y reconstruir la propia identidad, para tener la oportunidad de volver a crearse uno mismo ejerciendo un mayor control sobre la propia identidad.”

Comprender estos matices es, por tanto, el punto de partida indispensable para analizar si los mecanismos jurídicos actuales son realmente eficaces para poder garantizar el derecho al olvido en la era de la memoria total.

1.2. Justificación y relevancia social: La estigmatización algorítmica como barrera a la rehabilitación.

Este tema de investigación se eligió precisamente porque requiere de un análisis jurídico riguroso de cómo la indexación permanente de datos en Internet genera un impacto directo en los principios de reinserción social. La justificación del ¿Por qué? de este trabajo radica de una tensión fundamental en nuestra sociedad digital: el conflicto entre la memoria perpetua de internet y el derecho de las personas a una segunda oportunidad.

En el marco del Estado social y democrático de Derecho (Art.1 CE), el sistema legal no debe limitarse a castigar actos ilícitos; sino que también tiene la responsabilidad constitucional de garantizar la reinserción de las personas en la sociedad tras cumplir sus condenas.

⁸ ANDRADE, Norberto Nuno Gomes de (2012). «El olvido: El derecho a ser diferente... de uno mismo. Una reconsideración del derecho a ser olvidado». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet» IDP. Revista de Internet, Derecho y Política. N.º 13, pág. 67-83. UOC.

Por lo que este análisis se centra en tres pilares fundamentales que visibilizan la urgencia y relevancia de la cuestión: El conflicto constitucional, su impacto social y su colisión directa con el mandato de reinserción.

Desde una perspectiva constitucional, como hemos establecido, el problema radica en la colisión entre derechos fundamentales: Por un lado, el derecho a comunicar y recibir libremente información veraz del Artículo 20.1.d CE que legitima la existencia de archivos y hemerotecas digitales cumpliendo con una función esencial para la memoria histórica e interés público. Por otro lado, se encuentran los derechos a la reputación, la privacidad y la propia imagen del Artículo 18.1 CE, intrínsecamente ligados a la dignidad y al libre desarrollo de la personalidad del Artículo 10.1 CE.

El verdadero núcleo del conflicto no surge de informaciones falsas, sino de aquellas que, siendo veraces en su origen, pierden su relevancia pública con el paso del tiempo. La indexación permanente de estos datos por los motores de búsqueda, como Google, convierten hechos pasados en un continuo presente, planteándose en este caso si el interés informativo de un hecho justifica un perjuicio perpetuo asociado a la dignidad de una persona (Vivanco Martínez, A)⁹

Esta tensión jurídica se traduce en un problema social de primer orden, especialmente para colectivos vulnerables como analizaremos en este trabajo, los cuales son sometidos a una cadena perpetua digital que les bloquea segundas oportunidades.

Imaginemos a una persona que, hace más de una década, cumplió una condena por un delito y cuyos antecedentes penales han sido legalmente cancelados. Al buscar una nueva oportunidad laboral o intentar alquilar una vivienda por ejemplo, una simple búsqueda de su nombre en internet revela la noticia de su detención. Este rastro digital, obsoleto pero indeleble, genera un perjuicio que anula en la práctica la “segunda oportunidad” que el ordenamiento jurídico formalmente concede.

Este estigma digital choca formalmente con el mandato del Artículo 25.2 de la CE, que establece que las penas deben estar orientadas a la “reeducación y reinserción social”.

⁹ Ángela Vivanco Martínez, *El derecho al olvido y el eventual poder que tenemos sobre nuestra propia “historia”*, pp. 349–381.

Para colectivos vulnerables, como personas con antecedentes penales ya cancelados o que han superado procesos de adicción, la huella digital actúa como una sanción de facto no prevista por el legislador, que carece de límite temporal y obstaculiza el libre desarrollo de la personalidad del individuo, protegido por el artículo 10.1 CE.

Esta premisa encuentra respaldo jurisprudencial directo por el Tribunal Supremo. La Sentencia del Tribunal Supremo 545/2015, de 15 de octubre¹⁰ advierte que el tratamiento automatizado de estos datos provoca un “efecto estigmatizador e impidiendo su plena inserción en la sociedad”.

Por tanto, este TFG plantea el reto de analizar si el marco jurídico actual y los mecanismos de desindexación del artículo 17 del RGPD son verdaderamente eficaces para evitar que un pasado ya superado se convierta en una barrera insalvable para el desarrollo personal y profesional de las personas. De este modo, la investigación busca dar respuesta a la necesidad de hacer valer el mandato constitucional de reinserción social y la dignidad humana frente a la memoria perpetua de los algoritmos.

1.3. Objetivos y metodología de la investigación.

La presente investigación se propone como objetivo general analizar si el marco jurídico vigente ofrece una protección realmente eficaz de la dignidad humana y de la reputación online de las personas en proceso de reinserción social frente a la permanencia indefinida de datos obsoletos en internet, especialmente aquellos vinculados a antecedentes penales ya cancelados y datos sensibles relativos a la salud o a procesos de adicción superados.

Partiendo de esta premisa, el trabajo persigue varios objetivos específicos. En primer lugar, examinar el régimen de protección reforzada aplicable a los datos especialmente sensibles conforme al artículo 9 del Reglamento General de Protección de Datos, valorando el alcance de las garantías jurídicas existentes frente a la difusión permanente de información con elevado potencial estigmatizador.

¹⁰ Tribunal Supremo. Sala de lo Civil (Pleno). Sentencia núm. 545/2015, de 15 de octubre (Rec. 2772/2013). Ponente: Excmo. Sr. D. Rafael Sarazá Jimena. Fundamento de Derecho Sexto (ECLI:ES:TS:2015:4132).

En segundo lugar, analizar la evolución jurisprudencial del Tribunal Supremo, del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea en relación con la tensión existente entre la libertad de información y los derechos al honor, la intimidad, la protección de datos y el libre desarrollo de la personalidad.

Finalmente, la investigación pretende determinar si los actuales mecanismos de supresión y desindexación previstos en el artículo 17 RGPD resultan suficientes para garantizar de manera efectiva el mandato constitucional de reinserción social previsto en el artículo 25.2 de la Constitución Española.

Desde el punto de vista metodológico, el estudio adopta un enfoque dogmático-jurídico basado principalmente en el análisis crítico de normativa, doctrina científica y jurisprudencia relevante tanto nacional como europea. La investigación parte del examen de las principales resoluciones judiciales que han configurado el contenido y los límites del derecho al olvido digital, prestando especial atención a la STJUE de 13 de mayo de 2014 (asunto C-131/12, caso Costeja), por constituir los principales referentes en la construcción jurisprudencial de esta figura.

2. El Marco Constitucional: La Ponderación de Derechos Fundamentales

Para comprender la configuración jurídica actual del derecho al olvido y su papel en términos de garantía de la reinserción social en la era de la información, resulta imperativo analizar su evolución histórica y legal. Este derecho no surge como una creación legislativa espontánea, sino que nace como una respuesta dogmática y jurisprudencial frente a la pérdida de la inercia del olvido natural.

El anclaje de este derecho en nuestro ordenamiento jurídico se encuentra en el Artículo 18.4¹¹ de la Constitución Española, el cual establece que “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”. Este precepto se erige como el fundamento originario de la protección de datos en España, sentando las bases para evitar que la automatización de la información pudiera, en un futuro, lesionar la dignidad de la persona u obstaculizar su libre desarrollo.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales reconoce en su Preámbulo I¹² que “nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales”.

Los primeros desarrollos de este mandato fueron la Ley Orgánica 5/1992, de 29 de octubre (en adelante LORTAD), y posteriormente, la Ley Orgánica 15/1999, de 13 de diciembre (en adelante LOPD). Esta última, supuso un avance muy significativo, al consolidar los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), convirtiéndolos en las herramientas jurídicas iniciales para mitigar la difusión de datos ya obsoletos.

¹¹ Constitución Española. (1978). Artículo 18. *Boletín Oficial del Estado*, 311, de 29 de diciembre de 1978.

¹² Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Preámbulo, apartado I (BOE núm. 294, de 6 de diciembre de 2018).

No obstante, este marco normativo resultó insuficiente ante el cambio de paradigma tecnológico. Como advierte Mónica Arenas Ramiro¹³ “Frente a estos nuevos problemas, los conceptos jurídicos de privacidad o vida privada y sus mecanismos de protección se han quedado obsoletos y dejan de ser efectivos. En este orden de cosas se hace imprescindible reforzar el control sobre nuestros datos personales que, en último término, suponga proteger nuestra dignidad personal frente a estos nuevos peligros”.

Esta carencia facilitó la consolidación de la “vigilancia algorítmica” de Stefano Rodotà, un fenómeno donde, en palabras de Artemi Rallo Lombarte¹⁴ “La tecnología lleva a la humanidad a la memoria como principio general y al olvido sólo por defecto”.

Ante la inacción del legislador y la obsolescencia del marco normativo, la verdadera delimitación dogmática del Derecho al Olvido se configuró a través de la práctica jurisprudencial. El punto de inflexión a nivel internacional lo marcó la Sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014 (Asunto C-131/12), conocida como el caso Mario Costeja vs Google Spain.

Esta resolución fue disruptiva al establecer dos principios clave: en primer lugar, responsabilizó directamente a los motores de búsqueda del tratamiento de datos que realizan; En segundo lugar, fijó una regla de ponderación clara, estableciendo que, por lo general, los derechos a la privacidad y a la protección de datos del ciudadano deben prevalecer sobre el negocio de los buscadores y sobre el interés de terceros en rastrear información vinculada exclusivamente al nombre del afectado.

Precisamente por ello, el análisis exhaustivo de esta resolución, su impacto doctrinal y los criterios específicos de supresión de datos que de ella emanan serán objeto de un estudio en el Capítulo 4 de este trabajo, titulado «Análisis jurisprudencial: evolución y criterios de supresión».

¹³ Arenas Ramiro, M. (2015). Recensión de: Artemi Rallo Lombarte, *El derecho al olvido en Internet. Google versus España*. Teoría y Realidad Constitucional, (36), 650-657.

¹⁴ Rallo Lombarte, A. (2014). *El derecho al olvido en Internet: Del caso Google al Big Data*. Centro de Estudios Políticos y Constitucionales.

Trasladando este debate al ordenamiento jurídico español, la recepción de esta línea doctrinal fue desarrollada por el Tribunal Constitucional. La STC 58/2018, de 4 de junio de 2018 (Recurso de Amparo 2096-2016)¹⁵, se establece como el pronunciamiento de mayor relevancia, al vincular directamente el derecho al olvido con el mandato constitucional de la reinserción social, exigiendo a los medios de comunicación la implementación de técnicas de desindexación mediante códigos informáticos (noindex) y, estableciendo la tesis de que la pervivencia de la huella digital lesiva no puede devenir en una pena indefinida que vacíe de contenido el imperativo constitucional de reinserción social.

Finalmente, esta evolución jurisprudencial culminó con el reconocimiento normativo del derecho al olvido en el marco europeo y español. El Reglamento (UE) 2016/679 (RGPD)¹⁶, establece formalmente en su artículo 17 el “derecho de supresión” -derecho al olvido-, imponiendo la obligación de suprimir los datos cuando estos ya no sean necesarios para los fines que motivaron su tratamiento. Este marco europeo se ve complementado en España por la LOPDGDD¹⁷ (Ley Orgánica 3/2018), que dedica un título específico a los derechos digitales. En particular, el artículo 93 regula el derecho al olvido en las búsquedas de internet, permitiendo la desindexación de enlaces cuando la información sea inadecuada, excesiva o haya devenido obsoleta por el transcurso del tiempo y, asimismo, el artículo 94 extiende esta protección a los servicios de redes sociales.

No obstante, la efectividad real de esta facultad no depende únicamente de su reconocimiento formal, sino de su aplicación efectiva mediante una ponderación rigurosa con la libertad de información y el interés público. Solo así podrá evitarse que la memoria digital transforme el pasado en una carga permanente, incompatible con los valores fundamentales de la dignidad y el libre desarrollo de la personalidad de los individuos.

¹⁵ Tribunal Constitucional (Sala Primera). (2018, 4 de junio). Sentencia 58/2018. Recurso de amparo 2096-2016. ECLI:ES:TC:2018:58.

¹⁶ Parlamento Europeo y Consejo de la Unión Europea. (2016, 4 de mayo). Reglamento (UE) 2016/679. *Diario Oficial de la Unión Europea*, L 119, 1-88.

¹⁷ España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado, 294, 6 de diciembre de 2018.

2.2. El derecho a la información (Art. 20.1.d CE): Requisitos de veracidad y la pérdida de "relevancia pública" por el paso del tiempo.

La clave para resolver la tensión jurídica mencionada anteriormente reside en el estudio de los límites intrínsecos al propio derecho a la información, consagrado en el artículo 20.1.d de la Constitución Española. Dicho precepto reconoce y protege el derecho a “comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades”.

En relación con los límites intrínsecos y según establece la STS 12/2019 de 11 de enero de 2019: “Este derecho fundamental al olvido no es un derecho ilimitado - sostiene la doctrina constitucional-, porque, aunque la Constitución no establece expresamente límites específicos, con base en el principio de unidad de la Constitución, resultan aplicables los límites derivados del respeto a otros derechos fundamentales, entre los que tiene especial relevancia la libertad de información que proclama el artículo 20 de la Constitución”

Este derecho, recogido en nuestro texto constitucional dentro del Título I, constituye uno de los pilares básicos de una sociedad democrática, otorgándole un estatus jurídico y una protección reforzada que limita la actuación del legislador.

Según establece Luis Aguiar de Luque¹⁸ “el precepto impone unos límites a esa capacidad del legislador [...] en cuanto que ha de hacerlo con carácter general (no limitado al caso individual), debe citar el derecho fundamental y en ningún caso puede afectar al contenido esencial del derecho”.

Además permite a sus titulares ejercer su autonomía sobre los mismos, dotándolos de una robusta capacidad de resistencia frente a otros derechos concurrentes. Su cumplimiento se articula en una doble vertiente: la eficacia vertical y la eficacia horizontal.

¹⁸ Aguiar de Luque, L. (2004). Los límites de los derechos fundamentales. *Derecho y Realidad*, (3), 143–162.

Por un lado, la eficacia vertical amparada por los artículos 9.1 y 53.1 de la Constitución Española, obliga a los poderes públicos actuar bajo el límite de estos preceptos fundamentales; Y por otro, la eficacia horizontal, derivada también del artículo 9.1 CE, extiende este deber de respeto a la esfera privada, vinculando a los ciudadanos entre sí en relación con la protección del contenido constitucional.

Este derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión, garantiza la existencia de una opinión pública libre y plural. Sin embargo, su ejercicio no es absoluto, este debe coexistir con otros derechos fundamentales, como el honor, la intimidad y, de forma especialmente significativa en el entorno digital, la protección de datos personales. Por ello, la jurisprudencia ha consolidado que su ejercicio legítimo depende de la concurrencia de dos requisitos esenciales: la veracidad de los hechos y su relevancia pública, por lo que el análisis de cómo estos dos elementos se ven afectados por el paso del tiempo es fundamental para justificar la prevalencia del derecho al olvido (Martínez Martínez, N. 2019)¹⁹

Como se puede extraer de la lectura del Artículo 20.1 de la CE, este no ampara la difusión de rumores, intervenciones o hechos falsos. La veracidad se erige por lo tanto, como un presupuesto sine qua non para que la libertad de información goce de protección constitucional, exigiendo al informador un deber de diligencia en la contrastación de los hechos que comunica.

En el supuesto en que la información difundida es inexacta, el conflicto con los derechos de la personalidad se resuelve con mayor facilidad a favor del afectado ya que, la ausencia de veracidad despoja a la información de su principal justificación y activa con mayor intensidad el derecho al olvido. Un claro ejemplo es la STS 12/2019, de 11 de enero de 2019²⁰, que confirmó la procedencia de la desindexación de una noticia que atribuía a un funcionario público la condición de “cazador furtivo”, cuando en una resolución posterior se había demostrado la inexactitud de tal afirmación.

¹⁹ Martínez Martínez, N. (2019). El conflicto entre el derecho al olvido y la libertad de información de la prensa contenida en hemerotecas. *Derecho Privado y Constitución*, 34, 51-95

²⁰ Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección Tercera), Sentencia núm. 12/2019, de 11 de enero de 2019, R. Casación núm. 5579/2017, ponente Excmo. Sr. D. José Manuel Bandrés Sánchez Cruzat.

El alto tribunal concluye que “en este concreto supuesto debe prevalecer el derecho a la protección de datos personales del reclamante (que había ejercitado el derecho de cancelación de datos personales ante Google) frente a la libertad de información, teniendo en cuenta que la noticia que era objeto de difusión a través del buscador Google carecía de uno de los requisitos que deben concurrir para considerar legítimo el ejercicio de la libertad de información, cual es el de su veracidad, al ser inexactos los datos publicados”

Por tanto, la veracidad, vinculada al deber de diligencia, es el presupuesto esencial que valida la libertad informativa. Al faltar este requisito, la noticia pierde el amparo del artículo 20.1.d CE, lo que dota de pleno fundamento jurídico a las solicitudes de supresión o desindexación, al no existir un interés público legítimo en la difusión de datos no contrastados.

El verdadero desafío jurídico del debate sobre la cadena perpetua digital halla su núcleo cuando una información, a pesar de haber sido veraz en su origen, experimenta una erosión de su interés público debido al mero transcurso del tiempo. Si bien la relevancia social justifica la difusión inicial de una noticia, su disponibilidad ilimitada en la red (asociada de forma permanente a la identidad del individuo), puede convertirse en una injerencia desmedida en sus derechos de la personalidad.

La interpretación de este conflicto ha experimentado una evolución doctrinal sustancial: el criterio original, que priorizaba la integridad de las hemerotecas digitales como pilares de la memoria colectiva, ha dado paso a una postura más depurada. La jurisprudencia actual distingue con claridad entre la preservación del registro en su fuente original y la difusión universal indexada por motores de búsqueda, lo que permite la localización de datos personales fuera de su contexto original.

En este cambio de paradigma, la STC 58/2018, de 4 de junio²¹ establece que “una vez publicada la noticia en los medios de prensa por el interés que supone su carácter actual, el tratamiento automatizado de los datos personales de los

²¹ Tribunal Constitucional (Sala Primera). (2018, 4 de junio). Sentencia 58/2018. Recurso de amparo 2096-2016. ECLI:ES:TC:2018:58.

implicados en ella [...]va perdiendo su justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esas personas, carecen de interés histórico”.

La trascendencia de este pronunciamiento reside en que consolida una visión dinámica de la relevancia pública. En lugar de entender el interés social como un atributo inmutable de los hechos, el alto tribunal advierte que este es susceptible de decaer con el tiempo. Se establece cuando “reconoce que se trataba, ciertamente de hechos veraces pero que el paso del tiempo habría supuesto que el tratamiento de estos datos, vinculados a hechos pretéritos, sea inadecuado, no pertinente y excesivo para la finalidad del tratamiento”.

En este escenario de ponderación, cuando el factor cronológico, la falta de notoriedad del afectado y la inexistencia de un interés social persistente vacían de contenido la libertad informativa, los derechos a la protección de datos y al libre desarrollo de la personalidad recobran su primacía frente a una información que ha devenido en obsoleta. Por lo que, la aplicación del derecho al olvido, amparada en el artículo 17 del RGPD y el artículo 93 de la LOPDGDD, permite corregir este tratamiento desproporcionado.

De este modo, se evita que el entorno digital convierta hechos pretéritos en una vertiente de “estigmatización perpetua” (analizada en el apartado 1.2), consolidando el criterio de que el interés público de la información es una cualidad dinámica y no un atributo inmutable que legitime la indagación permanente de la vida privada.

2.3. El derecho al honor, la intimidad y el libre desarrollo de la personalidad (Arts. 18 y 10.1 CE) en el entorno digital.

En palabras de María Álvarez Caro²² “El derecho al olvido encuentra sus raíces en el derecho a la intimidad (the right to privacy en su denominación en inglés) y en el derecho a la protección de datos personales, pudiendo considerarse que el derecho al olvido deriva de ellos”.

²² Álvarez Caro, María, Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital, Madrid, Reus, 2015, p. 27.

(Egusquiza Balmaseda, M. 2023)²³ Históricamente, el origen del derecho a la intimidad se vincula al estudio pionero de Warren y Brandeis, “The Right to Privacy”, publicado en 1890 en la Harvard Law Review. Inicialmente esta noción de privacy se definía de forma restrictiva como el “derecho a ser dejado en paz”(the right to be let alone). Con el paso del tiempo, esta idea fue ampliándose y adaptándose a los nuevos escenarios sociales y tecnológicos, hasta convertirse en un elemento clave para hacer frente a los desafíos derivados del uso de tecnologías y sistemas informáticos. Su contenido se ha ido extendiendo progresivamente hasta integrarse plenamente en el ordenamiento jurídico europeo, especialmente bajo la protección del artículo 8 del Convenio Europeo de Derechos Humanos (CEDH), en relación con el derecho al respeto a la vida privada y familiar, domicilio y correspondencia.

Como hemos observado anteriormente, en el ordenamiento jurídico español, el derecho fundamental a la intimidad recogido en el artículo 18.1 CE se encuentra intrínsecamente ligado a la dignidad de la persona y al libre desarrollo de la personalidad (artículo 10.1 CE), constituyendo la base del Estado social y democrático de Derecho del artículo 1.1 de la Constitución Española.

Ante el incipiente, pero ya perceptible, avance de las nuevas tecnologías de la información, el constituyente optó por articular una fórmula de protección en el artículo 18.4 de la CE. Este precepto, se identifica como el origen del denominado habeas data²⁴ o “libertad informática”, sentando las bases para evitar que la automatización de la informática pudiera, en un futuro, lesionar la dignidad de la persona u obstaculizar su libre desarrollo (Pérez Luño, A. 1992)²⁵

El concepto del habeas data y “libertad informática”, según el Diccionario Panhispánico del Español Jurídico se entienden como:

²³ María Ángeles Egusquiza Balmaseda, *Olvido oncológico: protección de datos de salud y no discriminación*, Revista de Derecho, Empresa y Sociedad (REDS), núm. 22–23, Época II (2023), ISSN 2340-4647.

²⁴ Diccionario Panhispánico del Español Jurídico (DPEJ). Real Academia Española.

²⁵ Pérez Luño, A. E. (1992). *Del habeas corpus al habeas data. Informática y Derecho: Revista Iberoamericana de Derecho Informático*, (1), 153–161.

“Derecho a la propia intimidad informática, que confiere a su titular un derecho de control sobre los datos (acceso, rectificación y cancelación de los mismos)”

“La entonces llamada “libertad informática” se configura como “un derecho a controlar el uso de los datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención”.

No obstante, la escasa precisión del texto constitucional conllevó, durante décadas, una duda real sobre la naturaleza jurídica de este apartado. Existía una incertidumbre dogmática sobre si el Artículo 18.4 CE contenía un nuevo derecho sustantivo o si era una simple matización o garantía técnica del derecho a la intimidad.

Este precepto, en sus inicios, fue objeto de diversas sentencias del Tribunal Constitucional que lo interpretaban de forma reduccionista, entendiéndolo únicamente como una garantía del derecho a la intimidad de las personas frente a las agresiones tecnológicas.

Sin embargo, la insuficiencia de este enfoque ante la consolidación de la “sociedad del dato” impulsó una evolución doctrinal decisiva. El primer paso hacia la autonomía de este derecho se dio en la STC 254/1993, de 20 de julio de 1993²⁶, que si bien lo calificaba como un “instrumento de garantía”, también reconocía que era “en sí mismo, un derecho o libertad fundamental”. En cuanto a su citación literal, esta establece que:

“En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática».”

²⁶ Sentencia del Tribunal Constitucional 254/1993, de 20 de julio. Boletín Oficial del Estado, núm. 197, de 18 de agosto de 1993. Recurso de amparo 1.827/1990.

Todo y que el hito definitivo de independencia y concreción de su contenido en el ordenamiento jurídico español se alcanzó con la STC 292/2000, de 30 de noviembre de 2000²⁷, al reconocer de manera expresa, la existencia de un derecho fundamental a la protección de datos, fijándose por lo tanto como un derecho independiente y con carácter autónomo. La misma establece su contenido al mencionar que:

“el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.”

En el contexto de la sociedad de la información, esta autonomía es fundamental, pues como establece la jurisprudencia más reciente, ambos derechos operan en ámbitos no siempre coincidentes. Por lo que es imperativo no confundir el derecho a la protección de datos del artículo 18.4 CE con el derecho a la intimidad del artículo 18.1 CE. Según establece la reciente STS 1495/2024, de 19 de marzo²⁸:

“Aunque el derecho a la protección o reserva de los datos y el derecho a la intimidad tienen evidentes caracteres comunes, no todo acceso a datos protegidos constituye por sí misma una violación del derecho a la intimidad. Ambos derechos son manifestaciones del derecho al respeto de la vida privada [...] pero se desenvuelven en ámbitos que no son necesariamente coincidentes.”

Bajo esta premisa jurisprudencial, el Tribunal Supremo matiza la distinción con la protección de datos, señalando que el ámbito de tutela de esta última es significativamente más amplio.

²⁷ Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. Boletín Oficial del Estado, núm. 4, de 4 de enero de 2001. Recurso de inconstitucionalidad 1.463/2000, promovido por el Defensor del Pueblo.

²⁸ Tribunal Supremo. (2024). Sentencia núm. 398/2024, de 19 de marzo (ECLI:ES:TS:2024:1495; rec. 3855/2023). Id Cendoj: 28079110012024100383.

Mientras que la intimidad protege lo estrictamente reservado, el derecho fundamental a la protección de datos abarca cualquier información personal, sea esta íntima o no, siempre que su tratamiento por parte de terceros pueda tener un impacto en los derechos del ciudadano, ya posean estos naturaleza fundamental o no. Por ello, a pesar de la estrecha interconexión que guardan los derechos al honor, a la intimidad y a la protección de datos de carácter personal, la jurisprudencia les dota de una naturaleza jurídica autónoma y diferenciada como hemos observado en la STC 292/2000.

Trasladándolo al plano normativo, la Ley Orgánica 1/1982 de 5 de mayo de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen²⁹, es la encargada de materializar el derecho fundamental del artículo 18 CE. No obstante, esta creación legislativa deviene ineficaz, generando una clara distinción frente a intromisiones específicas de los medios de comunicación.

Esta insuficiencia radica en su incapacidad estructural para dar respuesta a las nuevas formas de vulneración de la privacidad en la era digital. Al haber sido elaborada para un contexto analógico y de intrusión mediática puntual, deviene ineficaz para captar las ilicitudes derivadas del tratamiento masivo y automatizado de datos personales, planteándose un conflicto entre el tratamiento algorítmico y la indexación automatizada de la información.

En sintonía, la interpretación extensiva del derecho a la intimidad permite identificarla con el principio de autodeterminación informativa, entendido como la facultad soberana del individuo para supervisar y verificar el tratamiento de su información personal por parte de terceros. Según establece María Ángeles Egusquiza³⁰ “la posibilidad de que informaciones pasadas del sujeto puedan ser suprimidas, o no tenidas en cuenta, a fin de evitar una discriminación o valoración negativa de la persona, en esta era del big data, conforme su raíz fundamental”.

²⁹ Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (1982). *Boletín Oficial del Estado*, (115), de 14 de mayo de 1982.

³⁰ Egusquiza Balmaseda (2023), *Olvido oncológico*, p. 18.

Bajo esta premisa, mientras que el derecho a la intimidad se orienta a la preservación reservada al individuo frente a publicaciones no consentidas, el derecho a la protección de datos halla su contenido esencial en un poder de disposición y control efectivo sobre su propia huella digital (Murillo de la Cueva, P.L. 2002)³¹.

Este dominio sobre la información personal se erige como un elemento esencial para garantizar que el sujeto pueda gestionar su identidad en el entorno digital, impidiendo que la difusión permanente de datos obsoletos desvirtúe su realidad actual y garantizando, en última instancia, el mandato de reinserción social y los derechos básicos del individuo en el ámbito social, así como su dignidad y libre desarrollo de la personalidad.

2.4. El concepto de "Hemeroteca Digital": Distinción jurídica entre la fuente original y la indexación en motores de búsqueda.

La transición de los archivos de prensa analógicos a las hemerotecas digitales ha transformado profundamente el acceso a la información, pero también ha originado un complejo debate en el que colisionan la memoria histórica y el derecho de las personas a no quedar ancladas a su pasado. Para comprender el alcance y los límites del derecho al olvido, es indispensable trazar una distinción jurídica entre el tratamiento de datos que realiza el editor de la hemeroteca digital (la fuente original) y el que lleva a cabo el gestor del motor de búsqueda (el indexador).

La Hemeroteca Digital según la Biblioteca Nacional de España³² “nace con la intención de convertirse en un referente para la investigación y consulta tanto de las revistas como de la prensa histórica española. Esta tiene como objetivo “la consulta y difusión pública a través de Internet del Patrimonio Bibliográfico Español conservado en la Biblioteca Nacional de España”.

³¹ Murillo de la Cueva, P. L. (2002). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta: Cuadernos de Derecho*, 20, 43-58.

³² Biblioteca Nacional de España. (s. f.). *Hemeroteca Digital*.

Esta cumple con una función social de primer orden: la preservación de la memoria colectiva. La existencia y accesibilidad de esta memoria se ampara en el derecho a comunicar y recibir libremente información veraz, consagrado en el Artículo 20.1.d) de la Constitución Española. Su finalidad trasciende la mera actualidad para convertirse en una herramienta fundamental para la investigación histórica y la formación de la ciudadanía (Martínez Martínez, N. 2019)³³

Consciente de esta función, el Tribunal Supremo adopta una postura protectora de la integridad de estos archivos. En su jurisprudencia, como se refleja en la STS 545/2015, de 15 de octubre de 2015³⁴, sostiene que las noticias pasadas no deben ser objeto de cancelación o alteración, argumentando que

“la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión (en el sentido amplio del art. 10 del Convenio de Roma, que engloba la libertad de información), que excluye las medidas que alteren su contenido eliminando o borrando datos contenidos en ellos, como puede ser la eliminación de los nombres de las personas que aparecen en tales informaciones o su sustitución por las iniciales”.

Esta doctrina sostiene que modificar la fuente original, eliminando nombres o datos, equivaldría a una forma de reescribir la historia, lo que podría suponer un sacrificio desproporcionado del derecho a la información. Por tanto, la responsabilidad de mitigar el daño que una noticia pueda causar no recae en el editor de la Hemeroteca, sino en quien universaliza su acceso: el motor de búsqueda. La distinción entre la fuente y el indexador da lugar a dos mecanismos de protección con efectos muy diversos: la supresión y la desindexación.

³³ Martínez Martínez, N. (2019). El conflicto entre el derecho al olvido y la libertad de información de la prensa contenida en hemerotecas. *Derecho Privado y Constitución*, 34, 51-95.

³⁴ Tribunal Supremo (Sala de lo Civil). (2015, 15 de octubre). *Sentencia núm. 545/2015*

A diferencia del editor que crea y publica el contenido, los motores de búsqueda como Google no generan contenido propio, su actividad consiste en rastrear, indexar y organizar una gran cantidad de datos disponibles en Internet para ofrecerlos a los usuarios en forma de resultados.

La STJUE de 13 de mayo de 2014³⁵ (Asunto C-131/12, caso Coteja) fue la encargada en determinar que los gestores de motores de búsqueda son responsables, al establecer que “el gestor del motor de búsqueda es quien determina los fines y los medios de esta actividad y, así, del tratamiento de datos personales que efectúa él mismo en el marco de ésta y, por consiguiente, debe considerarse «responsable» de dicho tratamiento”. Esta calificación como responsables, vincula su actividad directamente a las exigencias del marco legal europeo (RGPD) y español (Ley Orgánica 3/2018). La función de indexar nombres propios vinculados a fuentes externas supone una afectación significativa a los derechos a la intimidad y a la protección de datos, multiplicando la difusión de la información y confiriéndole un carácter generalizado.

Como bien establece la STJUE “procede poner de manifiesto que el tratamiento de datos personales llevado a cabo en el marco de la actividad de un motor de búsqueda se distingue del efectuado por los editores de sitios de Internet, que consiste en hacer figurar esos datos en una página en Internet, y se añade a él”.

Esta última, de acuerdo con el Artículo 52 de la Carta de los Derechos Fundamentales³⁶ (UE 210/C 83/02) respeto al alcance e interpretación de los derechos y principios, se ha consolidado como la solución jurídica más equilibrada y proporcional, permitiendo proteger la dignidad y privacidad de la persona, evitando que un hecho pasado la estigmatice indefinidamente, sin por ello censurar la fuente original ni eliminar la memoria histórica.

³⁵ Tribunal de Justicia de la Unión Europea (Gran Sala). (2014, 13 de mayo). *Sentencia en el asunto C-131/12*.

³⁶ Carta de los Derechos Fundamentales de la Unión Europea, 30 de marzo de 2010, *Diario Oficial de la Unión Europea* (2010/C 83/02).

Este derecho se encuentra explícitamente regulado en el Artículo 93. Derecho al olvido en búsquedas de Internet³⁷ de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que faculta a toda persona a solicitar a los motores de búsqueda la eliminación de enlaces cuando la información sea, entre otros supuestos, inadecuada, no pertinente o excesiva por el transcurso del tiempo.

Se concluye que la distinción entre la fuente original y el motor de búsqueda es la clave del derecho al olvido digital. Mientras que la hemeroteca se protege como un archivo de interés público cuya integridad debe preservarse, el motor de búsqueda es considerado un responsable del tratamiento de datos con la obligación de desindexar aquellos enlaces que, por el paso del tiempo y la pérdida de relevancia pública, causan un perjuicio desproporcionado a la dignidad y libre desarrollo de la personalidad del individuo del artículo 10.1 CE.

³⁷ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018). *Boletín Oficial del Estado*, (294).

3. La Reinserción Social frente a la Huella Digital

En el marco del presente capítulo, dedicado a la relación entre reinserción social y huella digital, conviene partir de la concepción actual de las finalidades de la pena. Desde esta perspectiva, se entiende que las penas privativas de libertad deben contar con mecanismos eficaces que permitan una verdadera reintegración de las personas condenadas en la sociedad, alejándose de una lógica exclusivamente punitiva basada en el castigo por el delito cometido.

La Constitución Española incorporó por primera vez una referencia expresa a los fines de la pena. Así, su artículo 25.2³⁸ establece que “Las penas privativas de libertad y las medidas de seguridad estarán orientadas hacia la reeducación y reinserción social y no podrán consistir en trabajos forzados”.

En cuanto al concepto de “reeducación y reinserción”, se aprecia que se trata de conceptos muy ambiguos, que requieren de una especial interpretación y delimitación para comprender con mayor exactitud el sentido que el constituyente quiso atribuir a esta finalidad de la pena (Zapico Barbeito, M. 2009)³⁹. El análisis de su alcance adquiere especial relevancia a la luz del surgimiento de las nuevas tecnologías y la consolidación del llamado “derecho al olvido”, que inciden directamente en las posibilidades reales de reintegración social de las personas condenadas.

La verdadera problemática surge, en palabras de Cécile de Terwange⁴⁰ cuando “la infalibilidad de la memoria total de Internet contrasta con los límites de la memoria humana [...] Gracias a su «efecto eterno», Internet preserva los malos recuerdos, los errores del pasado, los escritos, las fotos o los vídeos de los que nos gustaría renegar”.

³⁸ Constitución Española. (1978). Artículo 18. *Boletín Oficial del Estado*, 311, de 29 de diciembre de 1978.

³⁹ Mónica Zapico Barbeito (2009). *¿Un derecho fundamental a la reinserción social? Reflexiones acerca del artículo 25.2 de la CE*. AFDUDC, 13, 919–944, p. 921.

⁴⁰ DE TERWANGNE, Cécile (2012). «Privacidad en Internet y el derecho a ser olvidado/derecho al olvido». En: «VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet» [monográfico en línea]. IDP. Revista de Internet, Derecho y Política. N.º13, págs. 53-66. UOC

Por esto, este capítulo analizará como la memoria perpetua de internet colisiona frontalmente con el mandato constitucional de la reinserción social del Artículo 25.2 de la CE, la protección de datos de carácter sensible del Artículo 9 RGPD y la propia finalidad de cancelación de antecedentes, convirtiéndose así en un obstáculo inevitable para la dignidad y el libre desarrollo de la personalidad del Artículo 10.1 CE. En particular, el estudio se centrará en la protección de datos especialmente sensibles con especial atención a los relacionados con las adicciones y, en la tensión existente entre la cancelación administrativa de antecedentes y la persistencia indefinida de la información en internet, especialmente en el ámbito del acceso al empleo.

3.1. El mandato constitucional de reinserción (Art. 25.2 CE): Su aplicación extensiva más allá del ámbito penitenciario.

El derecho al olvido se vincula de manera intrínseca con el valor fundamental de la dignidad y el libre desarrollo de la personalidad del artículo 10 de la CE. Así pues, la cancelación de los antecedentes penales se configura como un instrumento orientado a posibilitar la plena reintegración social y jurídica del condenado, conforme al mandato establecido en el artículo 25.2 de la CE.

Según establece la STC 174/1996, de 11 de noviembre de 1996⁴¹ “No han de perpetuarse en el tiempo los efectos de conductas pasadas que ya no existen para el mundo del Derecho. Si, como es el caso, quien fuera condenado ha obtenido la rehabilitación [...] que extingue de modo definitivo todos los efectos de la pena [...] no se puede tomar en consideración su condena.

Estos antecedentes penales poseen la consideración de datos de especial sensibilidad, lo que justifica su inclusión en el Registro Central de Penados, un archivo de carácter no público sometido a estrictas limitaciones de acceso. Desde su configuración como registro reservado, se ha pretendido garantizar la protección del honor, la intimidad y la vida privada de las personas, evitando cualquier divulgación indiscriminada o no autorizada.

⁴¹ Tribunal Constitucional. (1996, 11 de noviembre). *Sentencia 174/1996* (Recurso de amparo 2.042/1992). BOE núm. 303, suplemento, 17 de diciembre de 1996.

Al respecto, la STEDH de 13 de noviembre de 2012 (asunto M.M. contra Reino Unido)⁴², puso de relieve la conveniencia de que los antecedentes penales sean objeto de olvido cuando la condena se remonta a un periodo suficientemente alejado, en la medida en que dicha información es considerada parte del derecho a la vida privada consagrado en el artículo 8 de la CEDH y artículo 12 de la Declaración Universal de Derechos Humanos.

En este contexto, la efectividad del mandato de reinserción social no solo depende de la limitación del acceso a los antecedentes penales, sino también del control sobre la difusión de datos especialmente sensibles y de la persistencia de información relativa a condenas pasadas en el entorno digital, cuestiones que serán analizadas en los siguientes apartados.

3.2. La protección reforzada de datos sensibles: El tratamiento de datos de salud y adicciones (Art. 9 RGPD).

(Egusquiza Balmaseda, M. 2023) Es en el marco normativo europeo, donde el derecho a la protección de datos se establece como un pilar fundamental de la sociedad que otorga cierta protección de la identidad del individuo. Este derecho se obtuvo tras un complejo desarrollo legislativo: En primer lugar se incluyó en el año 2000 en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea relativo a la “protección de datos de carácter personal” como un derecho fundamental con carácter autónomo e independiente. Mas adelante, tras su vinculación en el Tratado de Lisboa en 2007, acabó incorporándose en el Tratado de Funcionamiento de la Unión Europea en su artículo 16, de conformidad con el artículo 39 del Tratado de la Unión Europea.

En cuanto al ámbito normativo del Derecho a la Protección de Datos, su aplicación es válida a través del Reglamento (UE) 2016/679⁴³ “relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

⁴² Tribunal Europeo de Derechos Humanos (2012). *M.M. c. Reino Unido*, Sentencia de 13 de noviembre de 2012.

⁴³ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, L119, de 4 de mayo de 2016.

El Reglamento (UE) 2016/679 es la herramienta jurídica válida para establecer los diferentes sistemas de protección de datos personales al reconocer el grado de sensibilidad de la información (Dopazo Fraguío, M. P. 2018)⁴⁴. En este sentido, los datos relativos a la salud conforman una categoría de especial sujeción a un régimen de protección reforzada, dada la trascendencia de estos datos en la esfera íntima del individuo.

La regulación del derecho al olvido en materia de adicciones, aunque no ha sido objeto de un desarrollo doctrinal específico, debe encuadrarse dentro de la categoría del artículo 9 RGPD⁴⁵ (tratamiento de categorías especiales de datos personales). Esta categoría debe plantearse como una nueva vertiente que permita delimitar el alcance de las excepciones que contempla el artículo 17 del RGPD en relación con el tratamiento de los datos de la salud de la persona.

El artículo 9.1 del RGPD establece, con carácter general, la prohibición del tratamiento en relación con estos datos personales por conformar una de las principales categorías con un alto potencial de discriminación, al establecer que “quedan prohibidos el tratamiento de datos personales que revelen [...] datos relativos a la salud [...] de una persona física”.

De la lectura de este apartado, se extrae que los “datos relativos a la salud” ocupan un lugar destacado debido a su especial sensibilidad y al grave riesgo que su tratamiento indebido puede suponer para los derechos y libertades fundamentales de las personas (explicación detallada 2.1 – 2.2).

Como se desprende del análisis doctrinal, M^a Ángeles Egusquiza⁴⁶ confirma que la persistencia de esta información en el entorno digital puede tener consecuencias severamente perjudiciales, al señalar que:

⁴⁴ Dopazo Fraguío, M. P. (2018). La protección de datos en el derecho europeo: Principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos). *Revista Española de Derecho Europeo*, (68), 113–148.

⁴⁵ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento general de protección de datos), DOUE L 119, de 4 de mayo de 2016, art. 9.

⁴⁶ María Ángeles Egusquiza Balmaseda, *Olvido oncológico: protección de datos de salud y no discriminación*, Revista de Derecho, Empresa y Sociedad (REDS), núm. 22–23, Época II (2023), ISSN 2340-4647.

“La relevancia y transcendencia que podría tener el acceso y uso de esa información para la persona física. Desde la perspectiva personal, tales datos pueden influir sobre la imagen, la consideración o el juicio de valor social sobre el sujeto, al desvelar aspectos íntimos de su comportamiento”

“e implicar su discriminación con efectos relevantes en distintos ámbitos de la vida, los más significativos son la obtención de empleo o su mantenimiento por un futuro rendimiento”

Un ejemplo ilustrativo de este riesgo puede observarse en procedimientos de custodia de menores, donde la difusión de una adicción superada podría ser utilizada como elemento para cuestionar la idoneidad parental, aun cuando no exista evidencia actual que justifique dicha valoración.

En este contexto, la legislación ha comenzado a dar respuesta a situaciones específicas donde la persistencia de un historial clínico superado se convierte en una barrera infranqueable para la plena integración social y económica. El ejemplo más notable es el desarrollo del denominado “derecho al olvido oncológico”.

Este figura jurídica se implementó en España mediante el Real Decreto-Ley 5/2023, de 28 de junio⁴⁷. Esta disposición legislativa incorpora en su capítulo II “medidas para hacer efectivo el derecho al olvido en la contratación de seguros y productos bancarios de los pacientes de patologías oncológicas una vez transcurrido un determinado período de tiempo desde la finalización del tratamiento sin recaída”. Este marco jurídico impide que, transcurrido un plazo determinado, el historial oncológico de una persona pueda ser utilizado para discriminarla, especialmente en la contratación de seguros de vida o productos de consumo, intentando proteger a quien ha superado una enfermedad de un estigma perpetuo que no se corresponde con su realidad presente.

⁴⁷ España. (2023). *Real Decreto-ley 5/2023, de 28 de junio*. Boletín Oficial del Estado, 154, 29 de junio de 2023.

Según la disposición adicional quinta segunda, relativa a la no discriminación por razón de VIH/SIDA, por haber padecido un cáncer o por otras condiciones de salud, el plazo fijado se establece “una vez transcurridos cinco años desde la finalización del tratamiento radical sin recaída posterior.”

Partiendo de esta misma lógica protectora, extendida por la disposición adicional quinta a “otras condiciones de salud”, resulta jurídicamente defendible plantear, por analogía, la configuración de un derecho al olvido en materia de adicciones. Según establece Cristián López Acosta⁴⁸ “En las formulaciones del National Institute on Drug Abuse (NIDA), por su parte, no hay ambigüedades a este respecto, definiéndose la adicción como una enfermedad del cerebro crónica, con recaídas frecuentes, similar a lo que podría ser el asma, la diabetes o la enfermedad cardíaca (Branch, 2011)”.

Al respecto, al reconocerse su carácter patológico, se confirma que los datos relativos a las adicciones superadas (drogadicción, alcoholismo u otras dependencias) comparten con el historial oncológico su naturaleza de dato de salud sensible exigido por el artículo 9 del RGPD y, de manera aún más acentuada, su potencial estigmatizador.

Por lo que la persistencia en el entorno digital de esta adicción pasada, que fue veraz en su momento, se torna obsoleta e irrelevante una vez que el individuo ha completado un proceso de rehabilitación, pudiendo resultar contrario a los principios fundamentales del RGPD, en específico los regulados en el artículo 5.1 (apartados d y e) relativos a la exactitud y limitación del plazo de conservación, ya que dicha información (Egusquiza Balmaseda, M. 2023) deja de reflejar la situación actual del interesado y puede proyectar una imagen distorsionada y perjudicial.

No obstante, cabe cuestionar la incoherencia legislativa actual: mientras que el legislador ha blindado específicamente a quienes han superado un cáncer, mantiene a los rehabilitados de adicciones en una vulnerabilidad jurídica que depende de interpretaciones analógicas. Este sesgo de estigma sugiere que no todas las enfermedades se perdonan por igual, consolidando una discriminación indirecta que el sistema de protección de datos aún no ha resuelto con la contundencia necesaria.

⁴⁸ Cristián López Acosta, *Adicción a sustancias químicas: ¿enfermedad primaria o síntoma psicoanalítico?*, Praxis. Revista de Psicología, Año 13, N° 20, 2011, pp. 41–60.

Por ello, podría valorarse la conveniencia de articular un mecanismo similar que, tras finalizar el tratamiento de desintoxicación y transcurrido un plazo prudencial sin recaídas, permita al interesado ejercer su derecho de supresión o desindexación. Todo ello con el fin de evitar situaciones de discriminación y garantizar su efectiva reinserción social, en coherencia con los principios del Reglamento (UE) 2016/679 y con el mandato constitucional de dignidad y libre desarrollo de la personalidad.

3.3. La paradoja jurídica: La cancelación administrativa de antecedentes penales frente a la vigencia perpetua de la información en internet en el ámbito de acceso laboral.

(Díez Ripollés, J. 2016)⁴⁹ En el escenario actual nos hallamos ante una paradoja jurídica de difícil resolución, ya que “los registros policiales, penales y penitenciarios de personas condenadas, investigadas o sospechosas por delito ganan en exhaustividad y volumen, gracias —entre otros factores— a los nuevos medios electrónicos.”.

En el ámbito de acceso al empleo, la problemática del derecho al olvido adquiere una dimensión específica que no radica en la colisión abstracta entre derechos fundamentales (ya analizada en el capítulo anterior), sino en la ineficacia práctica de los mecanismos jurídicos diseñados para garantizar la reinserción social, específicamente en la persistencia de información relativa a condenas penales pasadas en el ámbito digital, provocando que terceros (incluidos empleadores) conozcan indirectamente estos antecedentes ya cancelados, generando un efecto excluyente en el acceso al trabajo

En este contexto, la institución de la cancelación de antecedentes penales se fundamenta en una premisa jurídica esencial: la temporalidad de la pena y el derecho del individuo a la reeducación y reinserción social del artículo 25.2 de la Constitución Española. Este mecanismo no se entiende como una mera formalidad administrativa, sino como una garantía para el individuo para evitar que este acto penal se convierta en una forma de exclusión social de carácter permanente.

⁴⁹ Díez Ripollés, J. L. (2015–2016). *El abuso del sistema penal*. Anuario de Derecho Penal, 141–159.

El Código Penal establece en su artículo 136.4⁵⁰ que “las inscripciones de antecedentes penales en las distintas secciones del Registro Central de Penados y Rebeldes no serán públicas”. Este precepto garantiza la limitación de acceso a estos antecedentes por parte de terceros, en conexión con los artículos 5 y 6 del Real Decreto 95/2009, de 6 de febrero, relativos al “acceso general a la información contenida en el Sistema de registros”.

No obstante, pese a la existencia de este principio de no publicidad, la realidad evidencia una tendencia contraria. Como señala Díez Ripollés, estos “antecedentes por condena son accesibles cada vez en mayor número y más fácilmente a instituciones no penales, empresas u organizaciones privadas y particulares.” Generando una tensión directa con los valores fundamentales a la vida privada y familiar y la libertad de expresión (véase capítulo 2).

Asimismo, el artículo 136.1 del CP reconoce que “los condenados que hayan extinguido su responsabilidad penal tienen derecho a obtener del Ministerio de Justicia, de oficio o a instancia de parte, la cancelación de sus antecedentes penales”. Desde una interpretación sistemática del ordenamiento, cabría entender que, una vez se produce la cancelación de estos antecedentes, debería limitarse su difusión, especialmente en los motores de búsqueda en coherencia con el derecho de “supresión” del artículo 17 del RGPD y el mandato constitucional del artículo 25.2 de la CE. Sin embargo, en la práctica se produce una clara disociación entre la realidad jurídica, en la que el antecedente penal ha sido cancelado, y la realidad digital, donde la información continúa siendo accesible de forma indefinida a través de motores de búsqueda.

Según establece Carmen Rocío Fernández⁵¹ “a pesar de que la cancelación de antecedentes penales constituye teóricamente un derecho del condenado, la inscripción registral de un sujeto condenado por un delito trae consigo consecuencias colaterales que, de alguna manera, sí afectan a los principios de proporcionalidad, necesidad y, sobre todo, a la reinserción social.”

⁵⁰ Código Penal (1995). *Ley Orgánica 10/1995, de 23 de noviembre*.

⁵¹ Fernández Díaz, C. R. (2024). *Antecedentes penales y exclusión social: Una mirada a España, a Europa y al Tribunal Europeo de Derechos Humanos en la era digital*. Revista de Derecho UNED, (33), 151.

(Rocío Fernández, C. 2024) Sobre estas consecuencias secundarias se pueden identificar claramente dos enfoques: en primer lugar, están las consecuencias formales, que abarcan sanciones, limitaciones o inhabilitaciones asociadas a los antecedentes con base legal, y en segundo lugar, se encuentran las consecuencias informales (que se analizarán por su relación con el objetivo de reintegración social), las cuales fomentan prácticas discriminatorias y excluyentes, creando barreras sociales sin soporte legal. Entre estas últimas, destaca de forma significativa la dificultad de acceso al empleo en el ámbito privado.

En esta línea, Elena Larrauri⁵² se pronuncia al respecto afirmando que la solicitud del certificado de antecedentes penales (CAP), se establece como una práctica frecuente y en aumento, para poder acceder a un empleo.

En España se exige carecer de antecedentes penales para “acceder a un puesto de funcionario público [...] y los funcionarios de prisiones [...] Pero también se aplica el Estatuto Básico del Empleado Público a jueces, profesores de Universidad, médicos de hospitales públicos o maestros. [...] Además se exige carecer de AP para trabajar, aun cuando sea sometido al régimen laboral en algunas instituciones Públicas [...] o profesiones reguladas”.

La Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales⁵³, establece en su artículo 10 que “El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal”.

⁵² LARRAURI, Elena. ¿En qué empleos se exigen los antecedentes penales? Actualización del artículo RECPC 13-09 (2011). *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2013, núm. 15

⁵³ España. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 294, de 6 de diciembre de 2018

De ello se desprende que, en ausencia de dicha habilitación, los empleadores no pueden acceder directamente a los registros oficiales, ya que supondría una vulneración del derecho fundamental a la protección de datos.

En este sentido, la problemática no radica en el acceso formal a los antecedentes penales por parte de empleadores, sino en la posibilidad de conocer hechos delictivos pasados a través de motores de búsqueda, generando que su persistencia temporal se prolongue cada vez más, como establece Carmen Rocío Fernández⁵⁴ debido a la “ampliación de los plazos de prescripción de delitos, de la cancelación o borrado de antecedentes, o de la dificultad de realizar estas últimas operaciones”. En la práctica, esta limitación puede dar lugar a conductas abusivas: en concreto, ante la imposibilidad de acceder directamente a dicha información, algunos empleadores trasladan esta carga al propio solicitante de empleo, exigiéndole que sea él quien obtenga y presente el certificado, lo que, en última instancia, desvirtúa la finalidad de la norma.

Esto conduce a una indudable revisión del sistema para buscar la manera de establecer límites ante esta prerrogativa de consulta de antecedentes penales para el acceso al puesto de trabajo. (Larrauri, E. 2011)⁵⁵. En los supuestos donde hay un peligro de amenaza inminente y grave, más allá de la ejecución de la pena, es el derecho penal quien debe encargarse de esa amenaza, en lugar de permitir que sean las empresas privadas las que verifiquen antecedentes penales, lo cual puede generar prácticas discriminatorias.

Se consuma plenamente la paradoja jurídica planteada: mientras el ordenamiento limita de forma estricta el acceso a los antecedentes penales (como refleja el artículo 10 de la LOPDGDD) y reconoce el derecho a su cancelación con el fin de garantizar la reinserción social, la realidad digital permite que esta información siga siendo accesible por vías indirectas. Así, sin que concurra una vulneración formal de la norma, los empleadores pueden conocer hechos delictivos pasados a través de motores de búsqueda, eludiendo en la práctica las garantías legales y generando consecuencias informales de carácter discriminatorio, especialmente en el acceso al empleo.

⁵⁴ Fernández Díaz, C. R. (2024). *Antecedentes penales y exclusión social: Una mirada a España, a Europa y al Tribunal Europeo de Derechos Humanos en la era digital*. Revista de Derecho UNED, (33), 151.

⁵⁵ LARRAURI, Elena. ¿En qué empleos se exigen los antecedentes penales? Actualización del artículo RECPC 13-09 (2011). Revista Electrónica de Ciencia Penal y Criminología (en línea). 2013, núm. 15

En definitiva, esta paradoja convierte la cancelación de antecedentes en una victoria pírrica. El Estado cumple formalmente con su deber administrativo de cancelación, pero por omisión, permite que los buscadores privados actúen como un registro paralelo e incontrolable, generando que esta inacción vacíe de contenido real el mandato de reinserción social del artículo 25.2 de la CE, reduciéndolo a una garantía formal que se rinde ante la persistencia de los algoritmos, prolongando de facto los efectos de la condena. En este contexto, el derecho al olvido se configura como un instrumento imprescindible para restablecer la coherencia del sistema, limitando la difusión de información que ha perdido su relevancia pública.

4. El origen de la doctrina: La STJUE de 13 de mayo de 2014 (Caso Costeja)

La Sentencia del Tribunal Europeo de Justicia de la UE de 13 de mayo de 2014⁵⁶, fue la encargada de establecer y delimitar el controvertido derecho al olvido (right to be forgotten en su denominación en inglés). Esta sentencia resuelve la cuestión prejudicial planteada por la Audiencia Nacional (Asunto C –131/12) en el procedimiento entre Google Spain S.L. “Google Inc.” y la Agencia Española de Protección de datos AEPD, Mario Costeja González.

En palabras de María Álvarez Caro⁵⁷ “este fallo judicial podría calificarse, si no como la sentencia más importante en materia de protección datos en la historia del TJUE, sin duda, como una de las más trascendentales en la materia.”

El 13 de mayo de 2014, el TJUE ante la cuestión prejudicial planteada por la Audiencia Nacional Española (AN), dictó sentencia en relación con la interpretación de varios preceptos de la Directiva 95/46 de Protección de Datos. En cuanto al origen del litigio, se entiende como el ejercicio por parte del Sr. Costeja del derecho de oposición de su datos personales contra el diario La Vanguardia y Google.

El origen del litigio se produce con la reclamación por parte del Sr. Costeja González contra la Agencia Española de Protección de Datos en el año 2010. Esta reclamación se fundamentaba en que cada vez que el recurrente (Costeja) introducía su nombre en el motor de búsqueda de Google, este mostraba en su lista de resultados dos vinculaciones al periódico La Vanguardia, donde aparecía indexado su nombre en el marco de una subasta inmobiliaria originada por deudas con la Seguridad Social.

El Sr. Costeja ante la negativa del ejercicio de este derecho por parte del buscador y el periódico, reclamó ante la Agencia Española de Protección de Datos (AEPD). Está estimó únicamente la prerrogativa contra Google, instando al buscador a adoptar las medidas oportunas para retirar los datos pertinentes de su indexado e imposibilitar el acceso del público a determinada información.

⁵⁶ Tribunal de Justicia de la Unión Europea. (13 de mayo de 2014). *Sentencia del Tribunal de Justicia (Gran Sala) en el asunto C-131/12, Mario Costeja González contra Google Spain SL y Google Inc.*

⁵⁷ Idem (Álvarez Caro, María)

No satisfechos con la decisión tomada por la AEPD, Google Spain y Google Inc. apelaron ante la Audiencia Nacional, que optó por presentar tres cuestiones prejudiciales al Tribunal de Justicia de la Unión Europea (TJUE). Dichas cuestiones, llevaron a la Gran Sala a realizar una interpretación de la Directiva 95/46/CE, centrándose principalmente en: Área territorial que abarca la mencionada directiva; El concepto de “tratamiento de datos personales” y “responsables del tratamiento” y; La posibilidad de solicitar al motor de búsqueda, en virtud de un supuesto derecho al olvido, la eliminación de información o datos relacionados con el interesado.

4.1. Análisis Jurisprudencial: Evolución y Criterios de Supresión

Sobre las cuestiones prejudiciales, la primera en plantearse es si la indexación de los motores de búsqueda debe considerarse “tratamiento de datos”. Al respecto Google (22) argumenta que su actividad no es fruto de ningún tipo de tratamiento, al establecer que “la actividad de los motores de búsqueda no puede considerarse tratamiento de los datos que se muestran en las páginas web de terceros que presenta la lista de resultados de la búsqueda, dado que estos motores tratan la información accesible en Internet globalmente sin seleccionar entre datos personales y el resto de información.”

El Tribunal de Justicia al respecto, considera lo contrario, estimando que la actividad que ejecuta Google si se enmarca dentro del concepto de “tratamiento de datos” establecido en la Directiva Europea, al declarar que (26) “la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un «tratamiento» de esta índole, en el sentido del artículo 2, letra b), de la Directiva 95/46”.

Se confirma este vertiente al declararse en la STJUE (28) que “al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, deben calificarse de «tratamiento» en el sentido de dicha disposición”

Por lo que se confirma que existe cierto activismo por parte de los motores de búsqueda sobre los datos que dispone y maneja, estableciéndose plenamente en el concepto de “tratamiento de datos personales” que contiene la Directiva Europea 95/46.

La segunda cuestión prejudicial que plantea la Audiencia Nacional conecta plenamente con el concepto del Derecho al Olvido, sugiriéndose hasta qué punto el motor de búsqueda tendría o estaría obligado a eliminar o desindexar vínculos o webs de sus resultados de búsqueda. Google se mantenía firme al considerar que, al no ser editor de contenidos (el que realmente publica en Internet), no tenía ninguna obligación bajo esta prerrogativa.

(63)“Google Spain y Google Inc. consideran que, en virtud del principio de proporcionalidad, cualquier solicitud que tenga por objeto que se elimine información debe dirigirse al editor del sitio de Internet de que se trate, ya que éste es quien asume la responsabilidad de publicar la información, quien puede examinar la licitud de esta publicación y quien dispone de los medios más eficaces y menos restrictivos para hacer que esa información sea inaccesible.”

Ante esta negativa por parte de Google, el TJUE es firme al establecer un factor primordial: el efecto multiplicador que provoca Internet sobre una publicación. A este respecto, cabe señalar que (47) “habida cuenta de la facilidad con que la información publicada en un sitio de Internet puede ser copiada en otros sitios y de que los responsables de su publicación no están siempre sujetos al Derecho de la Unión, no podría llevarse a cabo una protección eficaz y completa de los interesados si éstos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de sitios de Internet.”

En cuanto a si existe algún tipo de obligación por parte de Google en cuanto a la eliminación de estos vínculos, se confirma que la persona afectada sí que podrá dirigirse al gestor del motor de búsqueda para que ejecute la eliminación de estos datos, como sugiere la STJUE (77)“el interesado puede dirigir las solicitudes con arreglo a los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 directamente al responsable del tratamiento, que debe entonces examinar debidamente su fundamento y, en su caso, poner fin al tratamiento de los datos controvertidos”.

Previamente, aclarar que el TJUE establece una clara delimitación en la obligación de los editores de contenido informativo de suprimir publicaciones originales, estableciendo cierta responsabilidad a los motores de búsqueda para evitar una difusión desproporcionada. La tercera y última cuestión prejudicial, se establece en lo relativo a si se puede solicitar al administrador del motor de búsqueda que, elimine estos datos perjudiciales, o simplemente porque esta persona desea que estos datos sean “olvidados” por el mero transcurso del tiempo.

Según se establece en la STJUE (90) se “confieren derechos a los interesados únicamente a condición de que el tratamiento controvertido sea incompatible con dicha Directiva o por razones legítimas propias de su situación particular, y no por la mera razón de que consideren que este tratamiento puede perjudicarles o deseen que los datos objeto de ese tratamiento caigan en el olvido.”

Por lo que queda claro que a Google, ante esta prerrogativa, no se le podrá exigir que suprima estos datos, ya que considera ilógico que la simple petición de una persona de olvidar una información justifique la obligación de eliminación por parte del motor de búsqueda.

En esta línea, la STJUE (93) se contrapone por completo insistiendo que sí que procederá la eliminación del contenido comprometido de los motores de búsqueda, justificándose en que “incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Éste es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido.”

Por lo que la resolución de estas solicitudes, se proyectarán bajo el marco normativo europeo, ponderado los criterios mencionados en la sentencia al margen referenciada, entre ellos: la adecuación, exactitud y relevancia. Haciendo especial hincapié en el tiempo transcurrido o su carácter excesivo respecto al fin que la motiva (93).

“Con arreglo a los artículos 7 y 8 de la Carta [...] como se desprende del apartado 81 de la presente sentencia, que estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona”.

Eso sí, en el caso de tratarse de personajes públicos “sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate.” Por lo que, en el supuesto de persona cuya actividad profesional es de carácter público, esta exigencia se verá mucho más limitada por el principio de información pública.

En conclusión, la sentencia del TJUE de 13 de mayo de 2014 marcó un hito sin precedentes al reconocer que los motores de búsqueda son responsables del tratamiento de datos personales. El "Caso Costeja" no solo definió el derecho al olvido, sino que estableció que los derechos fundamentales a la privacidad y protección de datos deben prevalecer, por norma general, sobre el interés económico del buscador y el interés público de acceder a información que ha quedado obsoleta o carece de relevancia, protegiendo así la dignidad del individuo frente a la memoria perpetua de internet.

A pesar de la victoria jurídica, la implementación práctica de este derecho revela una profunda asimetría de poder. El sistema actual es puramente reactivo al trasladar toda la responsabilidad de acción y prueba al eslabón más débil ya que, es el ciudadano quien debe detectar la vulneración, identificar los enlaces y rogar a corporaciones multinacionales mediante formularios (Anexo A) la retirada de la información. Para colectivos más vulnerables o personas sin recursos jurídicos, este proceso se convierte en un muro infranqueable, puesto que, mientras las corporaciones utilizan algoritmos para indexar y lucrarse, el ciudadano debe luchar manualmente para desindexar.

CONCLUSIONES

El análisis desarrollado en el presente trabajo permite concluir que la denominada “cadena perpetua digital” constituye uno de los principales desafíos jurídicos derivados de la consolidación de internet y del actual modelo de memoria permanente en el entorno digital. La evolución tecnológica ha provocado que el olvido deje de operar de manera natural, permitiendo que hechos pertenecientes al pasado continúen siendo accesibles de forma inmediata y condicionen indefinidamente la vida personal, social y profesional de los individuos, aun cuando hayan perdido toda relevancia pública.

La hipótesis inicial planteada en esta investigación queda confirmada. La permanencia ilimitada de datos personales sensibles en la red, especialmente aquellos vinculados a antecedentes penales cancelados o a procesos de adicción ya superados, produce una afectación directa sobre derechos fundamentales como la dignidad, el honor, la intimidad y el libre desarrollo de la personalidad reconocidos en los artículos 10 y 18 de la Constitución Española. La capacidad de internet para conservar y difundir información de manera permanente termina generando una forma de estigmatización continua que resulta difícilmente compatible con el mandato constitucional de reinserción social previsto en el artículo 25.2 CE.

CONCLUSIÓN PRIMERA: El estudio realizado ha permitido comprobar que el verdadero conflicto jurídico no aparece frente a informaciones falsas o ilícitas, sino respecto de noticias que fueron veraces y legítimas en el momento de su publicación, pero cuyo interés público desaparece con el paso del tiempo. La evolución jurisprudencial del Tribunal Supremo, del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea ha ido configurando una concepción dinámica de la relevancia pública, rechazando que esta pueda mantenerse indefinidamente únicamente por la existencia de herramientas tecnológicas capaces de conservar la información de forma permanente.

Las resoluciones analizadas evidencian que el derecho al olvido no pretende eliminar la historia ni alterar la integridad de las hemerotecas digitales. Su finalidad consiste en limitar la difusión masiva e indiscriminada de información obsoleta cuando ésta deja de responder a un interés general y pasa a afectar de forma desproporcionada a los derechos de la persona afectada.

La diferenciación jurídica entre la fuente original y la indexación realizada por los motores de búsqueda constituye el elemento esencial para alcanzar una ponderación equilibrada entre libertad de información y protección de datos personales, por lo que la desindexación aparece así como una medida razonable que permite preservar la memoria colectiva sin convertir el pasado de una persona en una condena permanente.

CONCLUSIÓN SEGUNDA: El análisis del marco normativo europeo y español permite concluir que el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018 han supuesto un avance significativo en la protección de la identidad digital, especialmente a través del artículo 17 RGPD y del artículo 93 LOPDGDD. Sin embargo, también se ha constatado que la efectividad práctica de estos mecanismos continúa presentando limitaciones importantes debido a la complejidad de la ponderación entre derechos fundamentales y a la ausencia de criterios uniformes plenamente consolidados. El reconocimiento formal del derecho al olvido no resulta suficiente cuando la permanencia de información obsoleta continúa proyectando consecuencias negativas sobre la vida presente del individuo.

CONCLUSIÓN TERCERA: La problemática adquiere una especial intensidad en relación con los datos de salud y las adicciones. El carácter especialmente sensible de esta información, protegido por el artículo 9 RGPD, evidencia el elevado potencial discriminatorio que puede derivarse de su difusión permanente en internet. La persistencia de datos relacionados con enfermedades o dependencias ya superadas puede afectar gravemente al acceso al empleo, a las relaciones sociales o incluso al ejercicio de determinados derechos personales y familiares.

El desarrollo normativo del denominado “derecho al olvido oncológico” representa un precedente relevante que permite plantear la necesidad de extender mecanismos similares a otros supuestos relacionados con adicciones rehabilitadas o patologías superadas. La investigación realizada permite sostener que la difusión permanente de información relativa a procesos de drogadicción, alcoholismo u otras dependencias puede llegar a vaciar de contenido los principios de rehabilitación y reinserción social cuando dichos datos dejan de responder a la realidad actual del individuo.

Todo ello evidencia que la protección de datos sensibles no debe limitarse únicamente al ámbito sanitario o administrativo, sino que debe proyectarse también sobre el funcionamiento de los motores de búsqueda y sobre la permanencia de la huella digital en internet, especialmente cuando esta información posee un evidente potencial estigmatizador.

CONCLUSIÓN CUARTA: Desde una perspectiva crítica, puede apreciarse que el ordenamiento jurídico actual continúa ofreciendo una respuesta insuficiente frente a los efectos reales de la permanencia digital. Aunque el derecho al olvido ha supuesto un avance indiscutible en la protección de los derechos fundamentales, su aplicación práctica sigue siendo limitada, lenta y, en muchos casos, dependiente de la capacidad del propio afectado para iniciar procedimientos complejos frente a grandes plataformas tecnológicas.

La protección de la dignidad y de la reinserción social no debería descansar exclusivamente sobre la iniciativa individual de quien ya se encuentra en una situación de vulnerabilidad social o reputacional. Del mismo modo, resulta criticable que el desarrollo tecnológico y la capacidad de recopilación masiva de datos hayan avanzado a una velocidad muy superior a la capacidad de adaptación del Derecho. La realidad digital actual evidencia que las garantías tradicionales de cancelación de antecedentes o rehabilitación jurídica resultan insuficientes cuando la información permanece accesible de manera indefinida mediante motores de búsqueda y sistemas automatizados de indexación.

Puede apreciarse, además, que gran parte del modelo económico digital continúa sustentándose en la acumulación permanente de datos personales y en la maximización de su difusión, lo que provoca una tensión constante entre intereses económicos, libertad informativa y protección efectiva de los derechos fundamentales. Esta situación demuestra que la regulación actual todavía presenta importantes carencias para impedir que internet termine funcionando, en la práctica, como un mecanismo de sanción social perpetua.

CONCLUSIÓN FINAL: Los objetivos planteados al inicio de este trabajo han quedado cumplidos. El estudio realizado ha permitido analizar la protección reforzada de los datos sensibles prevista en el artículo 9 RGPD, examinar la evolución jurisprudencial relativa al conflicto entre libertad de información y derechos de la personalidad, así como valorar la suficiencia de los mecanismos de desindexación regulados en el artículo 17 RGPD para garantizar el mandato constitucional de reinserción social.

Todo ello permite concluir que, aunque el ordenamiento jurídico ha avanzado considerablemente en la protección de los derechos digitales, todavía persisten importantes dificultades para evitar que la memoria permanente de internet genere situaciones de exclusión, discriminación o estigmatización prolongada.

El derecho al olvido se ha convertido en una garantía imprescindible dentro del actual entorno digital, en el cual una sociedad democrática no puede permitir que la tecnología convierta errores pasados, enfermedades superadas o condenas extinguidas en elementos permanentes de identificación social.

BIBLIOGRAFÍA BÁSICA

Legislación

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 281, de 24 de noviembre de 1995.

Constitución Española. *Boletín Oficial del Estado*, 311, de 29 de diciembre de 1978.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (1982). *Boletín Oficial del Estado*, 115, de 14 de mayo de 1982.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (2018). *Boletín Oficial del Estado*, 294, de 6 de diciembre de 2018.

Real Decreto-ley 5/2023, de 28 de junio. (2023). *Boletín Oficial del Estado*, 154, de 29 de junio de 2023.

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. *Diario Oficial de la Unión Europea*, L119, de 4 de mayo de 2016.

Jurisprudencia

Carta de los Derechos Fundamentales de la Unión Europea, 30 de marzo de 2010, *Diario Oficial de la Unión Europea* (2010/C 83/02).

Sentencia del Tribunal Constitucional 254/1993, de 20 de julio. *Boletín Oficial del Estado*, núm. 197, de 18 de agosto de 1993. Recurso de amparo 1.827/1990.

Tribunal Constitucional. (1996, 11 de noviembre). *Sentencia 174/1996* (Recurso de amparo 2.042/1992). BOE núm. 303, suplemento, 17 de diciembre de 1996.

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre. *Boletín Oficial del Estado*, núm. 4, de 4 de enero de 2001. Recurso de inconstitucionalidad 1.463/2000, promovido por el Defensor del Pueblo.

Tribunal Constitucional (Sala Primera). (2018, 4 de junio). Sentencia 58/2018. Recurso de amparo 2096-2016. ECLI:ES:TC:2018:58.

Tribunal de Justicia de la Unión Europea. (2014, 13 de mayo). *Sentencia Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (Asunto C-131/12).

Tribunal Europeo de Derechos Humanos (2012). *M.M. c. Reino Unido*, Sentencia de 13 de noviembre de 2012.

Tribunal Supremo. Sala de lo Civil (Pleno). Sentencia núm. 545/2015, de 15 de octubre (Rec. 2772/2013). Ponente: Excmo. Sr. D. Rafael Sarazá Jimena. Fundamento de Derecho Sexto (ECLI:ES:TS:2015:4132).

Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección Tercera), Sentencia núm. 12/2019, de 11 de enero de 2019, R. Casación núm. 5579/2017, ponente Excmo. Sr. D. José Manuel Bandrés Sánchez Cruzat.

Tribunal Supremo. (2024). *Sentencia núm. 398/2024, de 19 de marzo* (ECLI:ES:TS:2024:1495; rec. 3855/2023). Id Cendoj: 28079110012024100383.

Doctrina

Aguiar de Luque, L. (2004). Los límites de los derechos fundamentales. *Derecho y Realidad*, (3), 143–162.

Álvarez Caro, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*. Madrid: Reus.

Ángela Vivanco Martínez. El derecho al olvido y el eventual poder que tenemos sobre nuestra propia “historia”, pp. 349–381.

Agencia Española de Protección de Datos (AEPD). Derecho al olvido.

Agencia Española de Protección de Datos (AEPD). (2020). Informe 0057/2020 sobre el contenido del derecho al olvido previsto en el artículo 17 del Reglamento (UE) 2016/679 y el artículo 93 de la Ley Orgánica 3/2018. Gabinete Jurídico de la AEPD.

Arenas Ramiro, M. (2015). Recensión de: Artemi Rallo Lombarte, El derecho al olvido en Internet. Google versus España. Teoría y Realidad Constitucional, (36), 650–657.

Biblioteca Nacional de España. (s. f.). Hemeroteca Digital.

DE TERWANGNE, C. (2012). “Privacidad en Internet y el derecho a ser olvidado/derecho al olvido”. En VII Congreso Internacional Internet, Derecho y Política. Neutralidad de la red y otros retos para el futuro de Internet. IDP. Revista de Internet, Derecho y Política, n.º 13, 53–66.

Díez Ripollés, J. L. (2015–2016). El abuso del sistema penal. Anuario de Derecho Penal, 141–159.

Dopazo Fraguío, M. P. (2018). La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. Revista Española de Derecho Europeo, (68), 113–148.

Egusquiza Balmaseda, M. Á. (2023). Olvido oncológico: protección de datos de salud y no discriminación. Revista de Derecho, Empresa y Sociedad (REDS), 22–23.

Egusquiza Balmaseda, M. Á. (2023). Olvido oncológico, p. 18.

- Fernández Díaz, C. R. (2024). Antecedentes penales y exclusión social: una mirada a España, a Europa y al Tribunal Europeo de Derechos Humanos en la era digital. *Revista de Derecho UNED*, (33), 151.
- Fernández Martínez, N. (2019). El conflicto entre el derecho al olvido y la libertad de información de la prensa contenida en hemerotecas. *Derecho Privado y Constitución*, 34, 51–95.
- Guichot, E. (2019). El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español. *Revista de Administración Pública*, 209, 45–92.
- Jiménez-Castellanos Ballesteros, I. (2019). “El conflicto entre el derecho al olvido digital del pasado penal y las libertades informativas: las hemerotecas digitales”. *Revista de Derecho Político*, (106), 141–142.
- Larrauri, E. (2013). ¿En qué empleos se exigen los antecedentes penales? *Revista Electrónica de Ciencia Penal y Criminología*, (15).
- López Acosta, C. (2011). Adicción a sustancias químicas: ¿enfermedad primaria o síntoma psicoanalítico? *Praxis. Revista de Psicología*, 13(20), 41–60.
- Martínez Martínez, N. (2019). El conflicto entre el derecho al olvido y la libertad de información de la prensa contenida en hemerotecas. *Derecho Privado y Constitución*, 34, 51–95.
- Moreno Bobadilla, Á. (2020). “El olvido previo a Internet: los orígenes del actual derecho al olvido digital”. *Cuestiones Constitucionales*, n.º 43, 200.
- Murillo de la Cueva, P. L. (2002). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta: Cuadernos de Derecho*, 20, 43–58.
- Pérez Luño, A. E. (1992). Del habeas corpus al habeas data. *Informática y Derecho*, (1), 153–161.

Rallo Lombarte, A. (2014). El derecho al olvido en Internet: del caso Google al Big Data. Madrid: Centro de Estudios Políticos y Constitucionales.

Rodotà, S. (2014). El derecho a tener derechos (J. M. Revuelta, Trad.). Editorial Trotta.

Zapico Barbeito, M. (2009). “¿Un derecho fundamental a la reinserción social? Reflexiones acerca del artículo 25.2 de la CE”. AFDUDC, 13, 919–944.

ANEXOS

Anexo A: Formulario para ejercer el derecho de supresión.

Este formulario para ejercer el derecho de supresión podrá presentarse ante el responsable del tratamiento (empresa o entidad que esté tratando sus datos).

EJERCICIO DEL DERECHO DE SUPRESIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO.

Nombre / razón social: Dirección de la Oficina / Servicio
ante el que se ejercita el derecho de supresión:
nº, C.Postal, Localidad, Provincia,
Comunidad Autónoma

DATOS DEL AFECTADO O REPRESENTANTE LEGAL.

D./ D^a., mayor de edad, con
domicilio en, nº, Localidad
....., Provincia, C.P., Comunidad
Autónoma con D.N.I., y, con correo
electrónico, por medio del presente escrito ejerce el derecho de supresión,
de conformidad con lo previsto en el artículo 17 del Reglamento UE 2016/679, General de
Protección de Datos (RGPD).

SOLICITA

Que se proceda a la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la supresión practicada.

Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Agencia Española de Protección de Datos.

Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique su supresión.

Se recomienda que acompañe al presente formulario un escrito en el que exponga de manera detallada todos los datos que permitan identificar el objeto de su pretensión.

En, a de de 20

Firmado: